

169 سلسلة محاضرات الإمارات

مستقبل الاستخبارات في القرن الحادي والعشرين

مارك بيردسول



مركز الإمارات للدراسات والبحوث الاستراتيجية

بسم الله الرحمن الرحيم

تأسس مركز الإمارات للدراسات والبحوث الاستراتيجية في 14 آذار/ مارس 1994، بوصفه مؤسسة مستقلة تهتم بالبحوث والدراسات العلمية للقضايا السياسية والاقتصادية والاجتماعية، المتعلقة بدولة الإمارات العربية المتحدة ومنطقة الخليج العربي على وجه التحديد، والعالم العربي والقضايا الدولية المعاصرة عموماً.

من هذا المنطلق يقوم المركز بإصدار «**سلسلة محاضرات الإمارات**» التي تتناول المحاضرات، والندوات، وورش العمل المتخصصة التي يعقدها المركز ضمن سلسلة الفعاليات العلمية التي ينظمها على مدار العام، ويدعو إليها كبار الباحثين والأكاديميين والخبراء؛ بهدف الاستفادة من خبراتهم، والاطلاع على تحليلاتهم الموضوعية المتضمنة دراسة قضايا الساعة ومعالجتها. وتهدف هذه السلسلة إلى تعميم الفائدة، وإغناء الحوار البنَّاء والبحث الجاد، والارتقاء بالقارئ المهتم أينما كان.

سلسلـة محاضرات الإمــارات

- 169 -

مستقبل الاستخبارات في القرن الحادي والعشرين

مارك بيردسول



تصدر عـن

مركـز الإمــارات للـدراسـات والبحــوث الاستــراتيجيــة

هذا الإصدار مستند أساساً إلى نص المحاضرة التي ألقيت في مقر المركز يوم الأربعاء الموافق 1 مايو 2013، ولا يعبر محتواه بالضرورة عن وجهة نظر المركز.

الطبعة الأولى 2014

ISSN 1682-122X

النسخة العادية ISBN 978-9948-14-824-1

النسخة الإلكترونية ISBN 978-9948-14-825-8

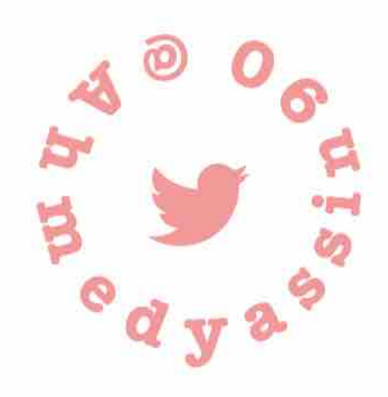
توجه جميع المراسلات إلى رئيس التحرير على العنوان التالي:

سلسلة محاضرات الإمارات، مركز الإمارات للدراسات والبحوث الاستراتيجية

ص. ب: 4567
أبوظبي، دولة الإمارات العربية المتحدة

هاتف: +9712-4044541
فاكس: +9712-4044542

E-mail: pubdis@ecssr.ae
Website: http://www.ecssr.ae


@Ahmedyassin90

مقدمة

ما هي الاستخبارات؟ كثيرون من الناس يعتقدون أن "الاستخبارات" ببساطة مصطلح عام يدل على المعلومات. ولكن الأمر ليس بهذه البساطة، لأن الاستخبارات أكثر أهمية من ذلك بكثير. إن عملية الاستخبارات هي محصلة جمع بيانات خام أو معلومات من مصادر مختلفة، وفي مجالات مختلفة. وإن الفئات الأساسية لطرق جمع المعلومات الاستخباراتية تُصنّف كالآتي:

HUMINT: الاستخبارات البشرية

ELINT: الاستخبارات الإلكترونية

COMINT: استخبارات الاتصالات

SIGINT: استخبارات الإشارات

IMINT: استخبارات الصور

OSINT: استخبارات المصادر المفتوحة

MASINT: استخبارات المقاييس والآثار

GEOINT: الاستخبارات الجيوفضائية

TECHINT: الاستخبارات الفنية/ التقنية

FININT: الاستخبارات المالية

هذه القائمة ليست شاملة، بل يوجد عناصر وفئات أخرى كثيرة من أنماط الاستخبارات. وهناك إضافة جديدة تتسق مع الموضوعات المذكورة أعلاه وهي **الاستخبارات السايبرية** التي يتم جمعها من الفضاء الإلكتروني CYBINT. وبصورة مشابهة، تظهر عبارات ومصطلحات جديدة بين الحين والآخر مع تطور طرق جمع المعلومات. **فالاستخبارات الجوية والبرية والبحرية والفضائية** جميعها تندرج ضمن فئات طرق جمع المعلومات. والطريقة الأكثر إثارة للجدل بشأن الحصول على المعلومات الاستخباراتية وتأمينها، غالباً ما يُشار إليها بكلمة "التجسس". وربما تكون استخبارات المصادر المفتوحة OSINT أكبر مزوّد أو أكبر فئة، حيث تتيح إمكانية جمع المعلومات وتوفيرها، في حين أن الاستخبارات البشرية HUMINT غالباً ما تثبت أنها الفئة الأكثر أهمية. ولكن، بجهود هذه القنوات مجتمعة، فإن المعلومات التي يتم توفيرها وإرسالها عبر نقاط التجميع هذه تشكل شريان حياة الحكومة. ولا تكمن قيمتها بالضرورة في حجمها، بل في دقتها وأمانتها. وفور الحصول على المعلومات يمكن تحليلها، أو تقييمها، أو توزيعها، أو تصنيفها، أو رميها. وفي نهاية المطاف، تُستخدم من قبل الحكومات، ويمكن أن تعزز أو توجه أو تملي صناعة القرار التنفيذي في كل المجالات، بما في ذلك السياستان الخارجية والمحلية، والأمن، والاقتصاد، والبحوث، والتكنولوجيا، والمجالات العسكرية.

لذلك، فإن الاستخبارات تُعد ذات أهمية قصوى لدى جميع الحكومات، وهي سلعة ثمينة جداً. وفي عالم متغير ومحاط بالهواجس والشكوك، لا يمكن معرفة القيمة الحقيقية للاستخبارات إلا بعد اختبارها. فالاستخبارات ليست الميدان الوحيد للحكومة، ولكنها تُستخدم من قبل أطراف معنية بعملية صنع القرار. ومع ذلك، سأركز في هذه الورقة البحثية فقط على الاستخبارات التي تُطلب وتُستخدم من قبل الجهات الرسمية، وهذا يعني تحليل عالم الاستخبارات السرية، كما يُنظر إليه من قبل أجهزة ومؤسسات رسمية مثل الاستخبارات البريطانية "إم آي 6(MI6) "، ووكالة المخابرات المركزية الأمريكية "سي آي أيه" (CIA). ولم يكن هناك طلب على الاستخبارات في يوم من الأيام أكثر من الوقت الحالي؛ وهي الآن أكثر تعقيداً من أي وقت مضى، وهناك صعوبة أكبر في إدارتها اليوم. وعالم الاستخبارات مملوء بألغاز متنوعة، وغالباً ما يُساء فهمها من قبل الجمهور. ولكن الأحداث المهمة التي وقعت خلال العشرين سنة الماضية، مثل هجمات 11 سبتمبر 2001، وتفجيرات لندن عام (2005)، والهجمات الإرهابية في مومباي عام (2008) وبالي عام (2002) وأماكن أخرى، توضح سبب الحاجة الماسة إلى أن يكون لدى الحكومات منظومة استخبارات. كما أن هذه الأحداث وضعت مهنة الاستخبارات تحت نظر الجمهور. والإرهاب مجرد عنصر واحد تسعى أجهزة استخبارات العالم إلى الحصول على معلومات عنه، ولكن في الوقت الحالي يمكن أن يقال إن الإرهاب هو العنصر الأهم.

إن أجهزة الاستخبارات مثل "إم آي 6" تتألف من إدارات مكلفة بمهام مختلفة، تتنوع من مكافحة التجسس إلى مراقبة خطوط الملاحة البحرية

قبالة القرن الإفريقي. وهناك دول مثل الولايات المتحدة الأمريكية لديها منظومات استخبارات تضم عشرات الأجهزة التنفيذية الكبيرة والصغيرة ترتبط فيما بينها، وجميعها تلعب دوراً معيناً؛ من هيئة الموانئ، إلى مراكز الحدود، وأجهزة مكافحة التجسس، وجهاز الأمن الداخلي المعروف باسم مكتب التحقيقات الفيدرالي "إف بي آي" (FBI). ويرتبط بعضها بأجهزة الاستخبارات العسكرية مثل وكالة الاستخبارات الدفاعية التي تُدار من قبل البنتاجون. ويُلاحظ أن مجتمع الاستخبارات في الولايات المتحدة (USIC) ضخم جداً، ولديه القدرة على الرد بسرعة، والعمل على مستوى العالم، والتفاعل مع حلفاء الولايات المتحدة.[1] والولايات المتحدة ليست سوى لاعب واحد في هذه الصناعة المدهشة، ومعظم الدول الحديثة لديها منظومات استخبارات نشطة. ولكن الحجم الضخم لمنظومة الاستخبارات لا يكفل بالضرورة النجاح؛ إنما التشغيل الفعال، والتمويل، والقدرة على التكيف، وتوافر الموارد، والدعم الفني، والخبرة هي العوامل المهمة.

هدف الورقة البحثية

تُعدّ مهنة التجسس "ثاني أقدم مهنة" في العالم، وقد وُلدت من الحاجة الماسة لدى أسلافنا القدامى إلى معرفة ما يفعله -أو يحضر لفعله- الخصم أو العدو أو الجار. ولذلك كانت هناك منذ آلاف السنين مساعٍ للحصول على الاستخبارات واستخدامها، خاصة في أوقات النزاع. وتحاول هذه الورقة البحثية التنبؤ بملامح عالم الاستخبارات في العقود المقبلة من القرن الحالي. وفي الأوراق البحثية لا يمكن الاعتماد على الافتراضات المبسطة أو على

التخمينات حول مستقبل الاستخبارات، حيث يوجد الكثير من العوامل المتغيرة والمتأرجحة. ولكن، في الوقت ذاته توجد أدلة ومفاتيح للألغاز تظهر في أيامنا، وهناك اتجاهات ودروس من الماضي يمكننا تحليلها والاستفادة منها - كما توجد أحداث غيّرت مسار التاريخ - وتحليل هذه المعلومات يمكن أن يزودنا برؤية ثاقبة ومفيدة ومقنعة.

لمحة تاريخية

كان لي شرف حضور المؤتمر السنوي الثامن عشر لمركز الإمارات للدراسات والبحوث الاستراتيجية الذي انعقد في إبريل 2013 تحت عنوان «الحروب المستقبلية في القرن الحادي والعشرين».[2] وفي ذلك المؤتمر، قال أحد المحاضرين إن العصر الحديث للاستخبارات بدأ عام 1909. وهذا صحيح، حيث أنشأت المملكة المتحدة مكتب الخدمة السرية (SSB)، وكان موظفو المكتب بضع عشرات من رجال أجهزة الاستخبارات العسكرية والمدنية، والشرطة، وموظفي الخدمة المدنية. وبعد عدة سنوات تم تقسيم ذلك المكتب إلى جهازَين: "إم آي 5" (MI5) و"إم آي 6" (MI6)، والاسمان الصحيحان لهذين الجهازين هما: جهاز الأمن، وجهاز الاستخبارات السرية. ولكن عبر مئات السنين، كانت بريطانيا تدير شبكة استخبارات مفككة، وتحرك الجواسيس داخل المملكة المتحدة وفي الخارج، ولكن لم يكن لهذه الشبكة هيكل تنظيمي يُذكر.[3]

إن إنشاء جهازَي الأمن إم آي 5، وإم آي 6، وخاصة الأخير أعطى بريطانيا رؤية عالمية شاملة عن الأحداث والوقائع في كل أنحاء

الإمبراطورية. وعندما اندلعت الحرب العالمية الأولى عام 1914، تم تكليف جهاز الأمن إم آي 5 بمعالجة أنشطة التخريب والمؤامرات والتعامل مع جواسيس العدو داخل بريطانيا؛ بينما كان جهاز إم آي 6 يبذل قصارى جهده لجمع الاستخبارات في أوروبا. وقبل 100 عام اتضح أن امتلاك قدرات للاستخبارات الداخلية، وقدرات للاستخبارات الخارجية نموذج مفيد، وتم تبنّي هذا النموذج من قبل دول عديدة، ولا يزال مستمراً حتى الآن. وعلى سبيل المثال، إن الأمن الداخلي الروسي يخضع لسيطرة جهاز الأمن الفيدرالي (FSB)،[4] في حين يقوم جهاز الاستخبارات الخارجية الروسي (SVR)[5] بجمع الاستخبارات من الدول الأجنبية. ولا أرى سبباً يدعو إلى تغيير هذه المنظومة في المستقبل.

في ثلاثينيات القرن العشرين، ظهر تهديد جديد في الأفق، وهو النازية. وفي عام 1939، دخلت بريطانيا مرة ثانية في حرب مع ألمانيا. ولكن هذه المرة تم إنشاء جهاز استخبارات ميداني جديد في المملكة المتحدة، وقد أثبت هذا الجهاز جدارته وقيمته العالية وأنقذ ملايين الأرواح. وُلدت مدرسة الرموز والشيفرات الحكومية (GC&CS) من وحدة سرية في البحرية البريطانية لفك الشيفرات تُعرف باسم "الغرفة 40". وخلال الحرب، تم نقل جزء كبير من عمل تلك الغرفة إلى مكان آمن نسبياً في منتزه "بلتشلي بارك"، وهو مبنى خاص مقام على مساحة واسعة، على مسافة ساعة شمال لندن. وفي هذا المكان قام خبراء فك الشيفرة باعتراض شيفرات الاتصالات السرية الألمانية وفكها، وكان أشهرها شيفرة تُدعى "الشيفرة اللغز".[6] وتم تفكيك إشارات ألمانية كثيرة، الأمر الذي ساهم في تقصير أمد الحرب شهوراً عدة، وبالتالي

إنهاء الصراع في أوروبا. وبالطبع، تُعرف تلك المدرسة البريطانية اليوم باسم آخر هو مقر قيادة الاتصالات الحكومية(GCHQ) وهي أكبر جهاز للاستخبارات في بريطانيا، ويبلغ عدد العاملين فيها 5000 فرد.[7] إن الاتصالات وكل الجوانب التي تشملها جزء حيوي أساسي في منظومات الاستخبارات في هذا الزمن. وهذا الجزء المهم في جمع المعلومات يشهد تغيرات هائلة مع بدايات القرن الحادي والعشرين. وظهرت تقنيات اتصالات جديدة ساهمت في تسريع إيصال المعلومات وتقديمها للجهة المعنية، وأهمها على الإطلاق الإنترنت. والواقع أن أجهزة الاستخبارات، مثل قيادة الاتصالات الحكومية (GCHQ) في بريطانيا، ووكالة الأمن القومي في الولايات المتحدة، تواجه صعوبة كبيرة في المحافظة على قنوات اتصال آمنة.

ظهور قوات غير نظامية في جمع الاستخبارات

شهدت سنوات الحرب العالمية الثانية أيضاً ظهور نمط جديد من المؤسسات شبيه بأجهزة الاستخبارات، وهذه المؤسسة الجديدة أوجدت العديد من الفنون/ المهام المرتبطة بعمل الجواسيس، مثل وحدة تنفيذ العمليات الخاصة (SOE). وتم تكليف العملاء الذين يعملون في هذه الوحدة الجديدة من طرف رئيس الوزراء البريطاني ونستون تشرشل بإشعال النار في أوروبا، وقد نفذوا ذلك بالضبط.[8] وأصبح أولئك المنفذون خبراء في هدم المباني، والتخريب، والحرب النفسية. وقام فريق المخترعين في وحدة تنفيذ العمليات الخاصة بصنع أجهزة مبتكرة مثل **الشوكولاته المتفجرة،**

والجرذان المتفجرة، وقاموا بصناعة أغذية مسمومة، واستخدموا العديد من الحيل القذرة. وربما يكون أفضل وصف لتلك الأنشطة "الفنون السوداء أو السحر الأسود". وبالفعل أحدث أفراد فريق تنفيذ العمليات الخاصة (SOE) دماراً وفوضى في أوروبا. وفي ذلك الوقت، بدأت تلك المؤسسة استخدام أسلحة سرية ومعدلة، وأساليب جديدة للتخفي، وأدوات مبتكرة أصبحت ركيزة أساسية لتطوير الأجهزة والأدوات المستخدمة من طرف الجواسيس في هذه الأيام. وقد أُعجب الأمريكيون بتكتيكات وحدة تنفيذ العمليات الخاصة، ولذلك أنشأوا **مكتب الخدمات الاستراتيجية (OSS)** وكان مقره في لندن أيضاً. وبعد نهاية الحرب العالمية الثانية، تم تطوير مكتب الخدمات الاستراتيجية ليصبح مؤسسة ضخمة يعرفها معظم الناس اليوم باسم وكالة المخابرات المركزية (CIA).[9]

الحرب الباردة

تمخضت الحرب العالمية الثانية عن ولادة أجهزة استخبارات جديدة في كل أنحاء العالم. وعلى الرغم من إرساء الأمن في أوروبا وآسيا، فقد نشبت حرب جديدة، وهي الحرب الباردة بين المعسكر الغربي والاتحاد السوفيتي.[10] وطوال معظم العقود الأربعة التالية، كان هناك سلام مضطرب بين واشنطن وموسكو، وكان ذلك السلام دائماً موضع ارتياب. وشهدت تلك الفترة زيادة سريعة في جمع الاستخبارات؛ حيث كان كل من الطرفين يحاول بكل طاقته الحصول على معلومات عن أسلحة الطرف الآخر، ومخزوناته، والقوة البشرية لديه، وأهدافه الاستراتيجية. كما كانت فترةً حافلة بالتجسس،

والخائنين، والمنشقين، والجواسيس، والأيديولوجيا التصادمية. وأصبحت المخاطر أكبر مما كانت عليه خلال الحرب العالمية الثانية، لأنه في أي لحظة كان يمكن أن تتحول السماء إلى كتلة لهب، نظراً إلى أن كل طرف من الطرفين كان يمتلك القدرة على إطلاق ترسانة هائلة من الأسلحة النووية. ووُلدت مصطلحات جديدة في عالم الاستخبارات، مثل عبارات **التدمير المتبادل المؤكد (MAD)**. وهذا المصطلح أو الفلسفة يعكس بصورة صحيحة ما يمكن أن يحدث لكلا الطرفين، لو تم إطلاق أي هجوم نووي. كما أسفرت الحرب الباردة عن نشر مجموعة كبيرة من التكنولوجيات الجديدة مثل طائرات التجسس الأمريكية من طراز U-2 وطراز بلاكبيرد SR-71. وفي أوائل ستينيات القرن العشرين تم إطلاق أقمار صناعية في الفضاء، وكانت تلك بداية فصل جديد في عملية جمع الاستخبارات. وبالفعل كانت تلك بداية **عصر التجسس الإلكتروني**.

في أكتوبر 1962، اختارت موسكو تخزين بعض أسلحتها النووية عند صديق بعيد عن حدودها، وهو جار قريب جداً من حدود الولايات المتحدة، وهو دولة كوبا. ولكن طائرات الاستطلاع الأمريكية سرعان ما اكتشفت وجود سفن عدة سوفيتية، وكشفت حمولتها المشتبه فيها. وأعقب ذلك مواجهة (سياسية/ إعلامية) حادة استمرت 13 يوماً، عُرفت باسم "أزمة الصواريخ الكوبية".[11] وهددت الولايات المتحدة بمهاجمة السفن السوفيتية إذا رست في موانئ الجزيرة. وتراجعت موسكو، مثلما كان قد توقع بعض محللي الاستخبارات الأمريكيين. وربما يكون الرئيس جون كنيدي قد غامر في ذلك الموقف، ولكن موقفه كان مناورة ذكية جداً مبنية على تحليلات تم إعدادها من

قبل وكالات استخباراتية، مثل "سي آي أيه" ووكالة الأمن القومي الحديثة العهد حينذاك. وقد أثبتت تلك الحادثة أهمية التحليلات الاستخباراتية، وتنفس العالم الصعداء مرة ثانية. اليوم، بالطبع نعرف أن العلاقات بين الطرفين أفضل مما كانت بكثير. في صيف 2010، قام مكتب "إف بي آي" بتفكيك شبكة تجسس روسية كانت تعمل طوال معظم السنوات العشر الماضية. وبعد محادثات سرية، سُمح لأحد عشر جاسوساً بمغادرة أمريكا، مقابل استرجاع أربعة جواسيس غربيين كانوا مسجونين في روسيا؛ ومنهم سيرجي سكيربال، وهو عقيد في جهاز المخابرات العسكرية الروسية كان قد سُجن إثر إدانته بالتجسس لمصلحة جهاز "إم آي 5" البريطاني.[12] وقد حدثت تبادلات مشابهة عديدة خلال فترة الحرب الباردة، حيث كان كل طرف يقايض على الجواسيس الذين يقعون في قبضته. ومؤخراً في 15 مايو 2013، نشر جهاز الأمن الفيدرالي الروسي (FSB) صور اعتقال موظف في السلك الدبلوماسي الأمريكي يُدعى ريان فوجل. وتزعم موسكو أنه عنصر من وكالة المخابرات المركزية كان يعمل لتجنيد عميل روسي. وليس هناك شك في أن حوادث مشابهة ستحدث في المستقبل، مع أنها قد تكون أكثر سرية وحذراً.

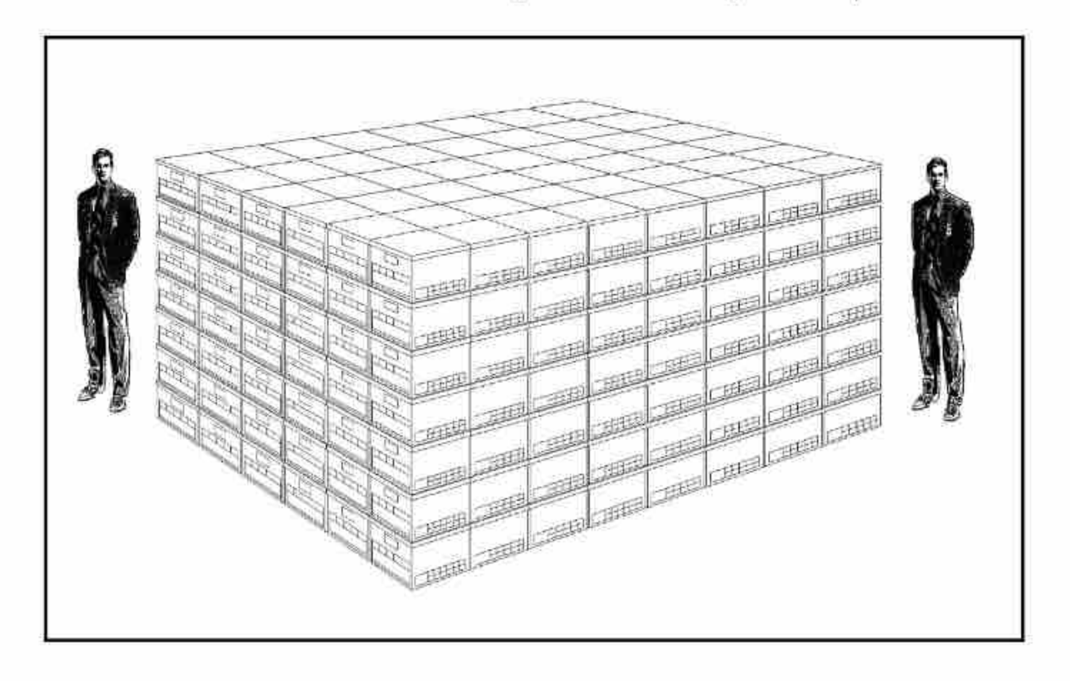
الأسرار وأمن المعلومات والتهديدات الداخلية

إن الأشخاص المكلفين بحماية أمن المعلومات الاستخباراتية يمكنهم اليوم أن يعتمدوا على مجموعة من المنتجات كانت مجرد حلم بالنسبة إلى أسلافهم. ولكن في عالم اليوم الحافل بالاتصالات المستمرة، والحواسيب والإنترنت، فإن حماية الأسرار أصبحت أكثر صعوبة من السابق. وقبل

ظهور منظومات تخزين المعلومات بواسطة الحواسيب، كانت المعلومات السرية تُخزّن بطرق يدوية، ولكنها كانت معرضة للمخاطر. في الثمانينيات، حُكم على محلل المعلومات في البحرية الأمريكية جوناثان بولارد بالسجن مدى الحياة، بعد إدانته بالتجسس لمصلحة جهاز الموساد الإسرائيلي.[13] وكان بولارد على مدى سنين طويلة يزوّد الإسرائيليين بنسخ من الملفات السرية المتعلقة بشبكة الاستخبارات العالمية التي تديرها الولايات المتحدة. ويمكن تخيل حجم المواد التي نَسخها يدوياً بواسطة آلة تصوير زيروكس، من خلال هذا الرسم التوضيحي (الشكل 1).

الشكل (1)

رسم توضيحي لكمية المواد التي نقلها جوناثان بولارد إلى الموساد



من خلال مقارنة عمل بولارد بعمل محلل الاستخبارات في القوات البرية الأمريكية برادلي مانناج، نجد أن: برادلي اعتُقل في مايو 2010 إثر

اكتشاف أنه قد حفظ ووزع 250 ألف برقية أمريكية، و500 ألف وثيقة متعلقة بالصراع في أفغانستان والعراق، ومقاطع فيديو، والكثير غيرها.[14] وفعل كل ذلك بطريقة مريحة من مكتبه بينما كان يخدم في العراق، وخلال لحظات. وكانت عواقب خيانته كبيرة، وتسببت خسارة هذه الكميات الهائلة من المواد الرسمية بإحراج كبير ليس للحكومة الأمريكية فقط، بل لدول أخرى أيضاً. والبرقيات الدبلوماسية تحتوي عادة على نصوص المحادثات الصريحة التي تحدث في الاجتماعات، والكثير منها يتضمن تعليقات وآراءً. وأبدت بعض الدول انزعاجها من التعليقات التي وُجدت في بعض البرقيات، كما شعرت بالحرج بسبب نشر العديد من المحادثات وعمليات التنسيق السرية على الإنترنت. كما وقعت أضرار بسبب نشر عشرات الاتصالات والمراسلات العسكرية الأمريكية التي تتضمن تفاصيل عن قرى في أفغانستان، حيث نجحت الاستخبارات العسكرية الأمريكية في بناء تعاون مع زعماء تلك القرى. ومن شبه المؤكد أن هذه الوثائق دُرست جيداً من قبل حركة طالبان، ولم يتطلب الأمر تحقيقات كثيرة من جانب حركة طالبان لكي تكتشف مَن كان يتحدث إلى مَن؟ أو مَن كان يقدم المساعدات لقوات التحالف. وهذه الحالات تعكس أهمية أمن المعلومات الاستخباراتية، أو أمن الاستخبارات.

في جميع أعمال الخيانة يكون هناك رد فعل عادة، وفي بعض الأحيان يكون هناك أشياء تتجاوز خسارة المعلومات. وعلى سبيل المثال، في حالة جورج بليك، وهو عنصر في جهاز إم آي 6 البريطاني خان بلاده، وكشف معلومات عن مشروع في غاية السرية مشترك بين وكالة المخابرات المركزية وجهاز إم

آي 6، وهو بناء نفق تجسس تحت برلين. وفي الحقيقة كان بليك جاسوساً لمصلحة جهاز كيه جي بي (KGB) السوفيتي، ومع أنه اعتُقل وسُجن فقد استطاع الهرب إلى روسيا. وقد احتفل مؤخراً بعيد ميلاده الـ(90)، ولكن أعماله أسفرت عن كشف وموت 40 عميلاً بريطانياً على الأقل.[15] وغالباً ما تكون هناك عواقب غير مكشوفة لعمل الخيانة، ولا تقتصر على الأمور المالية، التي يبدو أن أشخاصاً مثل برادلي يغفلون عنها. وهذه الحالات غالباً ما توصف بأنها "تهديدات عميل من الداخل". وهذا يقودنا إلى واحد من التحديات الأكثر إثارة وصعوبة بالنسبة إلى الذين يعملون في أمن الاستخبارات في القرن الحادي والعشرين، وهو الفضاء السايبري.

الفضاء السايبري

إن الاستخبارات المرتبطة بمشروعات تطوير التكنولوجيا المتقدمة شديدة الأهمية والحساسية. وهذا يجعلها معلومات مطلوبة من جانب الدول الأجنبية، وخاصة الدول المارقة. وأي خرق أمني في هذا القطاع قد يؤدي إلى خسارة سنوات من العمل، ويمكن أن يزود العدو بتصاميم متقدمة مشابهة. وهذا النوع من التجسس يسبب أضراراً كبيرة. ومع وجود العديد من الشركات المتعاقدة والمشروعات الحكومية التي تعتمد على الحواسيب والإنترنت، ليس هناك غرابة في كون التجسس السايبري قد أصبح مشكلة دولية كبرى. ربما لم يكن أولئك الذين يعملون في مجال الفضاء السايبري يتصورون أنه سيأتي وقت حيث يشكل فيه هذا الموضوع، العنصر الأكثر أهمية في عالم الاستخبارات. مما لا شك فيه أن شبكة الإنترنت غيرت العالم

والطريقة التي نسير بها في حياتنا. فالحكومات، والقوات المسلحة، ومراكز مراقبة حركة الطيران، والبنية التحتية، والصناعة، وشركات التكنولوجيا، وعالم الاستخبارات؛ جميعها بالفعل تعتمد بشكل كبير على الحواسيب. وهناك ملايين الأسرار والمشروعات الفائقة التقدم مخزنة الآن على أجهزة منظومات حاسوبية هي حتماً موصولة بشبكة الإنترنت. وهذا يعني أن هذه المنظومات جميعها معرضة للهجوم. وفي بريطانيا وحدها، تتعرض حواسيب الحكومات، والمنازل، والشركات الآن لأكثر من 100 ألف هجوم سايبري كل 24 ساعة. وهذا يساوي 44 مليون هجوم كل سنة، ويكبد الاقتصاد البريطاني خسائر هائلة تصل إلى 27 مليار جنيه إسترليني.[16]

على الرغم من تلقي التدريبات والإرشادات الكثيرة في مجال أمن الحاسوب، فإن من الحقائق المثيرة للاهتمام على مستوى العالم بأسره، أن كلمة السر الأكثر شيوعاً والمستخدمة من قبل مستخدمي الحواسيب هي كلمة "باسوُورد" Password نفسها. ويجب توفير قدر كبير من التعليم والتدريب، بالإضافة إلى جعل مستخدمي هذه المنظومات أكثر وعياً بمخاطر قراصنة الإنترنت. وتعد مخاطر الوضع أشد سوءاً في الولايات المتحدة. والمسؤولون في واشنطن يعترفون الآن بأن الحرب السايبرية، وانقطاع الاتصالات، والتجسس السايبري، تشكل أكبر تهديد لأمريكا. ويسعى البنتاجون وأجهزة الاستخبارات الأخرى إلى تطوير **القيادة السايبرية الأمريكية**، التي ستصبح جهازاً مستقلاً للاستخبارات يوظف آلاف المتخصصين.[17]

في بريطانيا ودول أخرى، هناك مشروعات مشابهة ولكنها أصغر بكثير. وهناك الكثيرون من الخبراء المتخصصين في الحقل السايبري يخشون

نتائج نقص التمويل لاتخاذ الإجراءات المضادة المناسبة، وغياب الاتفاقيات الدولية، حيث ستظل الحرب السايبرية تؤثر في جميع مستخدمي المنظومات الحاسوبية. وقد أوضحت واشنطن بكل صراحة أن التهديد الرئيسي يأتي من الصين، وهذا لأن جهاز الاستخبارات العسكرية الصيني يسعى إلى الاستيلاء على التكنولوجيا الأمريكية. وفي إبريل 2013، قالت شركة لوكهيد مارتن إنه قد تم إطلاق هجوم سايبري من الصين يستهدف النموذج الجديد الذي تصنعه الشركة من الطائرة الشبح المقاتلة ذات المهام المشتركة (JSF)؛ إلا أن الصين أنكرت التهمة. وتُعدّ مكافحة قراصنة الإنترنت تحدياً كبيراً حقاً بالنسبة إلى أجهزة الأمن في أيامنا هذه، وليس في مجال التجسس فقط. ويجب ألا يغيب عن البال أن البنية التحتية الحيوية في العديد من الدول، ومفاعلات الطاقة النووية، ومحطات المياه وشبكاتها، والغاز، والكهرباء، ووسائل النقل والمواصلات، والمنشآت العامة الضرورية الأخرى مثل المستشفيات، جميعها تعتمد على منظومات حاسوبية. وهذه المنظومات كلها تعرضت في السنوات الأخيرة لهجمات سايبرية، والمخاطر تتفاقم وتصبح أكبر باطراد.

وثمة مثال على مدى خطورة تعطل منظومة العمل، أو توقف التشغيل في هذه المنظومات الحساسة، وهو ما حدث في إيران. فقبل خمس سنوات أو ست قام خبراء في الحقل السايبري من الولايات المتحدة وإسرائيل[18] بتنفيذ مشروع فائق السرية بقصد إبطاء وتيرة العمل في البرنامج النووي الإيراني، الذي يعتقد بعض المحللين أنه يسير نحو إنتاج قنبلة نووية. وتم توليد فيروس يُدعى بالاسم الكودي ستوكسنت Stuxnet، وزُرع في منظومات

المراقبة الحاسوبية في أجزاء عديدة من البرنامج الإيراني. وهذا الفيروس أثر سلبياً في عمل 50 ألف حاسوب إيراني. وفي نهاية المطاف "تبخر" الفيروس، ولم يترك للمحللين فرصة لمعرفة تركيبته. ويمكن للمرء أن يتخيل حجم الفوضى والذعر إذا نجح القراصنة في تعطيل العمل في مفاعل نووي، أو إذا نجحوا في تعطيل حركة الطائرات، أو أي جزء في البنية التحتية الحيوية للبلاد المعنية. ومن اللافت للانتباه، أن الخبراء السايبريين في مجلة **آي سباي** *Eye Spy* يعتقدون أن ذلك الفيروس تم تحميله مباشرة في حاسوب واحد بطريقة يدوية بواسطة "وصلة تخزين" (USB) وليس عن طريق الإنترنت، وهذا يدل على أن عملاء الموساد استطاعوا الدخول إلى منشأة إيرانية تدير جزءاً من البرنامج النووي الإيراني. وهناك دول عديدة أيضاً تستخدم منظومات حاسوبية في عملية الانتخابات. وليس من المستحيل أبداً بالنسبة إلى أحد القراصنة المتمرسين، وخاصة بالنسبة إلى القرصان الذي يستهدف الدول الناشئة التي تعتمد على منظومات حاسوبية غير آمنة ولديها أمن سايبري ضعيف، أن يؤثر في نتيجة الانتخابات.

هناك حادثة أخرى مخيفة شدت انتباه مجلة **آي سباي**، وسببت اضطراباً في دوائر الاستخبارات، وهي موت رجل في مستشفى إيطالي عام 2010. حيث تم تغيير مستوى الجرعات الدوائية المنظمة بواسطة الحاسوب من قبل أحد القراصنة، وأدت الجرعة الجديدة إلى موت المريض. ويُعتقد أن هذه الحادثة هي أول **وفاة سايبرية** مسجلة.[19] ولكن مع أن الحادثة كانت عملية قتل تستهدف شخصاً معيناً، فقد تم تسجيل شهادة جوزيف ويس، مدير منظومات التحكم والشريك الإداري في شركة حلول التحكم التطبيقية،

في مارس 2009 أمام لجنة التجارة والعلوم والنقل في مجلس الشيوخ الأمريكي. وقال إن الشبكات التي تزود الطاقة الكهربائية لمنظومات التحكم الصناعية تعرضت للاختراق أكثر من 125 مرة في العقد الماضي. وذكرت التقارير أن إحدى هذه الحوادث أدت إلى وفيات بين الأمريكيين. وقال جوزيف ويس إنه شاهد تقريراً للحكومة الأمريكية بتاريخ 10 نوفمبر 2011 تحت عنوان: «هجوم سايبري على محطة مياه عامة في حي أمريكي». وقد أدى الهجوم السايبري إلى تعطيل مضخة المياه. وهذه الأمثلة تعكس إلى حد ما المخاطر التي يمكن أن تنتشر في عالم الفضاء السايبري.

هناك أدلة متزايدة توحي بأن بعض الأشخاص المشاركين في البحوث السايبرية مستهدفون أيضاً. ويمكننا القول إنه يوجد جانب أكثر ظلاماً وخطورة لهذا المجال الاستخباراتي الحيوي. وبالفعل يدور جدل حول وفاة شين تود التي حدثت مؤخراً، وهو خبير سايبري أمريكي يعمل في سنغافورة. ويعتقد والداه، ماري وريك تود، أنه قُتل بواسطة جهاز استخبارات أجنبي. وكان شين تود موظفاً لدى معهد الإلكترونيات الدقيقة (IME). وقد وُجد مشنوقاً في شقته في سنغافورة، بعد يومين فقط من تركه الشركة في يونيو 2012. وقال أفراد عائلته إنه تحدث عن مخاوف بشأن سلامته قبل موته.[20]

قبل عشرين عاماً، لم يكن الفضاء السايبري أو الإنترنت على لوائح الاستخبارات أو برامجها. اليوم تُعدّ الأنشطة السايبرية الحقل الاستخباراتي الأكثر أهمية. وفي السنوات المقبلة، ستظهر أجهزة ومنظومات حاسوبية أكثر تقدماً، والأجهزة التي نستخدمها اليوم ربما يُشار إليها بأنها "قطع أثرية

عتيقـة". ومـن غـير الحكمـة بالنـسبة إلى الحكومـات، أن تتجاهـل العـالم السايبري. إن عمليـات جمـع المعلومـات الاسـتخباراتية وتحليلهـا، ووضـع توقعات للمستقبل، تستفيد من المنظومات المرتبطة بالفضاء السايبري، ولكن كان واضحاً منذ البداية أن شـبكة الإنترنـت ستوجِـد مخـاطر كبـيرة، وعـالم الاستخبارات كان بطيئاً جـداً في اتخـاذ أي رد فعـل عـلى ظهـور الإنترنـت. ولذلك، ليس مستغرباً اليوم أن نجد أجهزة الاستخبارات قلقة بشأن "هجرة الأدمغة" إلى القطاع الخاص. فالمكافآت المالية في القطاع الخاص أكـبر بكثـير مما هي في القطاع العام. وهذه الهجرة تشكل معضلة كبيرة بالنسبة إلى أولئـك المكلَّفين باستقطاب كـوادر سـايبرية في المـستقبل، والمـسؤولين عـن التنميـة والدفاع، ويجب إيجاد حل سـريع لمعالجتها.[21]

إن خسارة المعلومات عبر مواقع شبكات التواصل الاجتماعـي مـصدر قلق أيضاً للمسؤولين عن مكافحة سـرقات الهوية والممتلكات. وعلى الرغم من وجود عدد كبير من الروابط الممتازة، يظل هنـاك مخـاطر. وهنـاك أنـاس كثيرون يقضون وقتاً طويلاً وهم يحاولون حماية معلوماتهم الشخصية، ولكن في الوقت نفسه هناك ملايين الناس يحمّلون البيانات الشخصية والمعلومـات المرتبطة بها على مواقع مثل "فيسبوك". وهنـاك مـسألة تثـير قـدراً أكـبر مـن القلق، وهي وجود أدلة كثيرة على أن عصابات الجريمة المنظمـة والجماعـات الإرهابية تستخدم مواقع التواصل الاجتماعي لجمـع المعلومـات واسـتغلالها وللتواصل مـع زميلاتهـا مـن التنظـيمات المـشابهة.[22] وفي إبريـل 2013، قـال جيمس كلابر، مدير مكتب مـدير الاسـتخبارات الوطنيـة (ODNI)، الآتي: «نظراً إلى اكتساب المزيد من الخبرات من قبل أطراف حكومية وأطراف غـير

حكومية في حقل الفضاء السايبري، فإن التنبيه إلى أهمية هذا الفضاء ووصفه بأنه تهديد عالمي لا يُعتبر مبالغة».[23] وقد صرحت الولايات المتحدة بأنها إذا تعرضت لهجوم سايبري على بنيتها التحتية يؤدي إلى حدوث وفيات أو تعطيل للخدمة، فهي تحتفظ لنفسها بحق الرد العسكري. وهذا قد يكون تحذيراً لما ينتظرنا في السنوات المقبلة من القرن الحادي والعشرين.

التلاعب الإلكتروني

وُلدت شبكة الإنترنت من رحِم برنامج عسكري أمريكي كان يهدف إلى تسريع الاتصالات. واليوم غالباً ما يُنظر إلى الرسائل الفورية ونقل المعلومات الحساسة على أنها مسألة ضرورية وشديدة الأهمية، وربما يكون هذا هو السبب الرئيسي الذي يدفع المعنيين إلى عدم إغلاق المنظومات والأجهزة، أو عزلها للحفاظ على أمنها. ومع أنه يمكن حماية جزء كبير من الشبكة، فإن بعض الأجزاء الأخرى تظل معرضة للخطر، وقد وُصفت هذه الأجزاء بأنها "بوابات الاستخبارات السايبرية".

ومثلما قدّمت الإنترنت الفوائد إلى عالم الاستخبارات، خاصة في مجالات معينة مثل البحوث، فهي تساعد أيضاً أولئك الذين يمارسون تجارتهم في بيئات الجريمة والإرهاب. وبدءاً من تصميم الرموز (الشيفرة) إلى إرسال رسائل بطرق سرية، وصولاً إلى تحميل أفلام دعائية، فإن الإنترنت تُستخدم على نطاق واسع من قبل الجماعات الإرهابية. لذلك، أعتقد أنه من الضروري أن يتم تزويد أجهزة الأمن بالوسائل اللازمة لتحليل هذه الاتصالات؛ بحيث يتم تحديد مكانها، واقتفاء أثرها، وتحديد هوية المرسل

والمتلقي. وهناك الكثيرون من مسؤولي الاستخبارات يؤيدون الجهود المبذولة لمراقبة حركة الاتصالات الإلكترونية، ويقولون إن السلامة العامة بالتأكيد أهم بكثير من هواجس الخصوصية. ويُعدّ القانون الأمريكي المقترح، وهو **قانون مشاركة الاستخبارات السايبرية (CISPA)**، خطوة جديدة لتهدئة مخاوف الجماعات المدافعة عن الحريات المدنية، والتي تعتقد أن القانون الجديد سيعطي مجتمع الاستخبارات في الولايات المتحدة (USIC) سلطات واسعة لمراقبة حركة جميع رسائل البريد الإلكتروني. ولكن هناك مشروعات مشابهة قيد الدراسة في بلدان أخرى. ففي بريطانيا، حذّر المدير العام السابق لجهاز إم آي 5، جوناثان إيفانز، من أن الجماعات الإرهابية تستخدم فعلاً بعض البرامج الإلكترونية التي هي خارج متناول أجهزة الأمن. وقال السير جوناثان، «إن الدخول إلى بيانات الاتصالات مسألة مهمة جداً».[24] وهذه المسألة تشكل مأزقاً بالنسبة إلى المسؤولين الحكوميين، بشأن المحافظة على التوازن بين الحريات المدنية والأمن القومي.

برنامج إيشيلون ECHELON

تتم مراقبة الاتصالات في أمريكا وبريطانيا من قبل وكالة الأمن القومي الأمريكي (NSA)، وجهاز قيادة الاتصالات الحكومية (GCHQ) البريطاني. وتستخدم أجهزة الاستخبارات مجموعة متنوعة من المنشآت العالمية (البرية، والبحرية، والجوية، والأقمار الصناعية) لجمع المعلومات الإلكترونية. وغالباً ما يتم تبادل البيانات الموجودة عن الأنشطة الإرهابية لدى الأجهزة الاستخباراتية مع دول صديقة. وليس هناك شك في أنه تم إحباط عمليات إرهابية بسبب جهود أجهزة الاستخبارات، ولكن التنظيمات القوية مثل

القاعدة والتنظيمات الفرعية التابعة لها تحولت أيضاً إلى طرق إلكترونية أخرى، وهذا يزيد من صعوبة التعرف على التهديدات التي تلوح في الأفق. ويستخدم تنظيم القاعدة تقنيات متنوعة من هواتف الأقمار الصناعية إلى أجزاء من الإنترنت، حيث يستحيل كشف التنظيم، وهذه التقنيات أصبحت على نحو متزايد خارج متناول وكالة الأمن القومي الأمريكي وجهاز قيادة الاتصالات الحكومية البريطاني. وطوال سنوات عدة كانت وكالة الأمن القومي الأمريكي وجهاز قيادة الاتصالات الحكومية البريطاني يعترضان الاتصالات الهاتفية لتحديد هوية الاتصالات المشتبه فيها. وتم تفعيل برنامج مخصص لهذه الغاية وأُطلق عليه الاسم الكودي "إيشيلون" ECHELON.[25] وكان النظام يرصد نحو 120 كلمة مفتاحية، مثل "متفجرات"، "قنبلة"، "هجوم"،... إلخ. ومع أن هذا البرنامج ربما لا يزال قيد التشغيل في صيغة أكثر تقدماً، وخاصة بشأن رصد اتصالات الهواتف المتحركة، فهناك قدر كبير من الاهتمام يتركز الآن بشكل طبيعي على شبكة الإنترنت. وهذا يأخذنا إلى موضوع مثير للاهتمام، وهذا الموضوع قد يُسهم أيضاً في كشف الاتجاه الذي ستسير فيه ما تُسمى **"عجلة الاستخبارات"** في السنوات المقبلة.

الاحترافية

إن الهجوم الأشد تدميراً في العالم حدث على الساحل الشرقي للولايات المتحدة الأمريكية في 11 سبتمبر 2001. وقد أُعطي الأمر بإطلاق الهجوم من قبل أسامة بن لادن، القائد المشهور لتنظيم القاعدة، وبتخطيط خالد شيخ محمد. وقد أظهر نجاح الإرهابيين في 11 سبتمبر نقاط ضعف ليس في نظام الاستخبارات الأمريكية فحسب، بل في أنظمة الاستخبارات في

بلدان أخرى يمكن أن تكون قد قدمت معلومات مساعدة لبعض المنفِّذين.[26] وما أعقب ذلك أصبح من التاريخ، ولكن إضافة إلى الفشل في دحر القاعدة في أفغانستان، فقد كان الهجوم على مقر أسامة بن لادن حافزاً لتفريخ شبكة عالمية من الخلايا والجماعات التي تواصل تنفيذ الأعمال الإرهابية المروّعة حتى الآن. وعلى الرغم من استمرار عمليات مكافحة الإرهاب في أفغانستان، وفي أجزاء من باكستان، وشمال إفريقيا، وبعض الدول في الشرق الأوسط، فإن تنظيم القاعدة لا يزال يشكل أكبر تهديد للسلم العالمي، ونادراً ما يفوّت أي فرصة لإعادة ابتكار نفسه وتشكيلها في الدول التي تعاني نقاط ضعف وتمر بمرحلة تغيير. فلا يزال لتنظيم القاعدة أتباع في سوريا وليبيا، ولكن بعض القياديين الكبار في التنظيم لديهم طموحات أوسع، وتشمل طموحاتهم إنشاء منظمة عبر الصحراء تمتد من المحيط الأطلسي حتى حدود الشرق الأوسط، وتشمل معظم شمال إفريقيا.

طوال عقد من الزمن ظل المحللون والمسؤولون في أوساط الاستخبارات يتساءلون كيف سيبدو العالم بعد موت أسامة بن لادن. ولكن للإجابة عن هذا السؤال، كان يجب على مسؤولي الاستخبارات أن يجدوه أولاً، وعندما وجدوه اكتشفوا أنه قد نجح في أن يبقى سالماً باستخدام أساليب التجسس التي ربما تكون مأخوذة من أجهزة استخباراتية عريقة. ومن مقر إقامته في أبوت أباد لم يستخدم أسامة بن لادن الإنترنت، وعندما كان يجري اتصالات بواسطة هاتف خليوي كان يستخدم مجموعة من الرموز السرية لكي يجعل المحادثة آمنة. واختار مكاناً قريباً من قاعدة للقوات المسلحة الباكستانية لأنه كان يعتقد أن الأمريكيين

لن يجرؤوا على مهاجمتها، حتى لو اشتبهوا في أنه يعيش هناك. وهناك مصطلح "**مختبئ في مرأى من الجميع**" يمكن أن يعبّر عن هذا الوضع. لقد أحاط أسامة بن لادن نفسه بعدد قليل من المراسلين المخلصين، الذين كانوا يسافرون آلاف الأميال لإيصال رسائله إلى الجهة المقصودة. وكان "زعيم الإرهاب" يخشى الاستخبارات الإلكترونية الأمريكية، ولذلك اختار العيش في عالم لا يمكن اختراقه بواسطة أجهزة استخباراتية، مثل وكالة الأمن القومي الأمريكي.

هناك أساليب للتجسس في أشكال عديدة، تتنوع من تحضير برامج المعلومات المضللة أو التضليل الإعلامي، واستخدام الحرب النفسية، إلى مهارات الجواسيس التي غالباً ما تُصور في أفلام هوليوود. وتُستخدم أساليب الجواسيس ومهاراتهم من قبل العناصر المكلَّفين بالمحافظة على أسرار معينة ومعلومات استخباراتية، ومما لا شك فيه أن هذه المهارات والأساليب تغيرت خلال الأعوام المئة الماضية، مع أن هدف الجاسوسية لم يتغير، **وهو الحصول على المعلومات.** لا تزال أساليب التجسس تُدرّس حتى اليوم في منشآت مثل "المزرعة" Farm التابعة لوكالة المخابرات المركزية في فيرجينيا، و"الحصن" Fortالتابع لجهاز إم آي 6 البريطاني في جنوب إنجلترا. وهناك أجهزة استخبارات عديدة في مختلف أنحاء العالم تدرّس المهنة. وهي مادة في غاية التعقيد تشمل استخدام معدات وتجهيزات، وفي معظم الحالات ترهق الأعصاب. ونادراً ما يشاهد الجمهور أساليب التجسس ومعداته، ولكن في عام 2006، ظهر جهاز اتصالات فائق التطور لدى إم آي 6 تم

تصنيعه ليبدو كصخرة أو حجر، واحتل العناوين الرئيسية في الصحف. وقد وضعت الصخرة في متنزّه في موسكو، وأتاحت للاستخبارات البريطانية تلقي رسائل وإرسالها إلى عدد من العملاء في المدينة. ولسوء حظ الاستخبارات البريطانية، تم تحذير جهاز الأمن الفيدرالي الروسي (FSB). وفي إحدى المرات تم التقاط صورة بواسطة كاميرا مراقبة مخبأة تابعة لجهاز الأمن الفيدرالي الروسي، لأحد عملاء الاستخبارات البريطانية وهو يركل الصخرة؛ لأنها لم تعمل كما ينبغي. وتم بث هذا الفيلم على شاشات تلفزيون الدولة، وسرعان ما نُشرت صور العملية التي كشفها الروس. ونتيجة لذلك تم كشف أسماء أربعة مسؤولين بريطانيين متورطين.

مع أن الأدلة كانت قاطعة، فقد نفت بريطانيا رسمياً أي تورط في القضية. ولم يعلق رئيس الوزراء البريطاني توني بلير على الحادثة. ولكن في وقت لاحق في يناير 2012، صرح جوناثان باول الذي كان يشغل منصب كبير موظفي مكتب رئيس الوزراء في "داوننج ستريت" في عهد بلير لإذاعة "بي بي سي": «كانت صخرة التجسس محرجة. ومن الواضح أن جهاز الأمن الروسي كان يعرف بأمرها منذ فترة، ولكنه كان يتكتم عليها لأغراض سياسية».[27] وبالفعل كان لتلك القضية آثار وانعكاسات سياسية، حيث كان الكرملين يسعى إلى تقليص نفوذ المنظمات غير الحكومية، وكانت موسكو تتهم بعض تلك المنظمات بالتواصل مع الغرب من خلال تجهيزات، مثل صخرة التجسس.[28]

استخدام التجسس أداةً إرهابيةً

إلى جانب الأمثلة الواضحة على عمليات التجسس، فقد استُخدمت أساليب التجسس في السنوات الأخيرة بقصد اختراق تنظيمات مثل القاعدة. ومن المهام الحساسة التي يمكن إنجازها عبر هذه الأساليب: تحذير السلطات المعنية بشأن هجوم إرهابي يجري التخطيط له؛ والتعرف على قنوات عمل الإرهابيين؛ وحركة نقل الأسلحة؛ واكتشاف طرق تمويل التنظيم؛ وكشف الملاذات والمنازل الآمنة والقياديين الكبار. ولكن هذه الأعمال لا تصلح للأشخاص ذوي القلوب الضعيفة، وإذا تم إلقاء القبض على هؤلاء العملاء ففي أغلب الأحيان تتم تصفيتهم.

وبالطبع سيستمر استخدام أساليب التجسس في القرن الحالي؛ ولا أرى أي سبب من أي نوع يوحي بأن واحدة من أقدم المهن في العالم ستنقرض فجأة. ولكن أساليب التجسس تتطور، كما أن التكنولوجيا، ووسائل الاتصالات، والسفر، جميعها أصبحت متاحة بشكل أكبر للذين يعملون في هذا الفن. ومن المؤسف أنه خلال العشرين سنة الماضية، بدأت تنظيمات إرهابية مثل القاعدة باستغلال الطرق والخدع نفسها التي تستخدمها أجهزة الاستخبارات. وهذا جعل عمل مسؤولي مكافحة الإرهاب أكثر صعوبة. ويمكن أن نجد مثالاً على ذلك في دولة الإمارات العربية المتحدة عندما كان تنظيم القاعدة على وشك إسقاط طائرة شحن بواسطة متفجرات مخبأة في علبة حبر الطابعات. ولو لم تعمل أجهزة الأمن الإماراتية بطريقة سريعة وبتعاون دولي فعال، لتمكّن الإرهابيون من تحقيق النجاح. وتتضمن أنشطة القاعدة أساليب متطورة لتهريب مواد كيماوية متنوعة على متن الطائرات،

وتصميم متفجرات بشكل ملابس داخلية يمكن تفجيرها في ثانية واحدة. وقد أصبح تنظيم القاعدة يمتلك مهارات وحيلاً متقدمة وذكية جداً في مخططاته. فهل هذه الأمثلة تندرج ضمن الفئة المعروفة "أساليب الجاسوسية"؟ بالطبع. إن التفجير الذي حدث في ماراثون بوسطن، في إبريل 2013، يثبت أنه بوساطة قدر قليل من الخيال وبتكلفة بضعة دولارات، يمكن إحداث ذعر وفوضى يستنزفان قدرات دولة بأكملها.[29]

في هجوم بوسطن، مات أربعة أشخاص، وأصيب 200 شخص آخرون بجروح وأضرار، وكانت إصابات بعضهم خطيرة. ولكن الهجوم أحدث أيضاً أثراً عميقاً على الأمن في أماكن أخرى في مختلف أنحاء أمريكا. وبعد بضعة أيام أُجري ماراثون لندن. وكان ذلك بالفعل مصدر قلق كبير لأجهزة الأمن؛ فهل كان هجوم بوسطن حلقة في عملية أوسع؟ في النهاية، تم تكثيف الإجراءات الأمنية بتكلفة بلغت ملايين الجنيهات الإسترلينية. ويُعدّ دحر تنظيم القاعدة عسكرياً أحد الخيارات المطروحة، ولكنني أخشى وأحذّر من أن إصرار الذين يعتنقون عقيدة القاعدة يمكن أن يجعل هذا الخيار شبه مستحيل.

كيف تعتزم الحكومات محاربة الإرهاب في السنوات المقبلة؟ هذه مسألة أنا ببساطة لا أستطيع التعليق عليها. التعليم قد يكون خياراً آخر، ولكن يوجد نموذج أستطيع التحدث عنه، وهو **الحرب الدموية التي خاضتها بريطانيا ضد الجيش الجمهوري الأيرلندي** في أيرلندا الشمالية، وهذه الفترة معروفة باسم "القلاقل".[30] نجح جهاز الاستخبارات إم آي 6 في إيجاد ما يُعرف في عالم الاستخبارات باسم "القناة الخلفية"، وهي قناة اتصالات

سـرية أدت إلى نقاش وحوار. وفي نهايـة المطـاف تـم إرسـاء الـسلام، وعـلى الرغم من أنه لا يزال هناك حالات وحوادث إرهاب في البلاد، فإن **"اتفاقيـة الجمعة العظيمة"** كما يُطلق عليها، لا تزال بشكل عام سارية ومطبقة.[31] ولكنّ الحوار مع تنظيم القاعدة بهذه الطريقة مستحيل، لأنه لا يوجد للتنظيم قيـادة مركزية. ربما يمكن إبرام اتفاقيات سـلام محلية ومناطقيـة، ولكـن القاعـدة مشكلة دولية، ولا يمكن حلها إلا بجهود المجتمع الدولي.

تغيير الأدوار

في عام 2007، قال جهاز الاستخبارات البريطـاني إم آي 5 إنـه يراقـب نحـو 2,000 عـضو نـشيطين في تنظـيم القاعـدة، وهـؤلاء يتلقـون دعـماً ومساعدات من شبكة محيطة من المتعاطفين يبلغ عددهم 20 ألـف شـخص. ومع أن بعض "أعضاء القاعدة" يعرفون زملاءهم، فـإن معظمهـم يعملـون كخلايا مستقلة. ومن الجدير بالملاحظة أنه خلال فـترة الحـرب البـاردة كـان 85٪ من أعـمال جهـاز الاسـتخبارات إم آي 5 تنحـصـر في حقـل مكافحـة التجسس، والاستخبارات المضادة. أما اليوم فـإن 85٪ مـن ميزانيـة الجهـاز البريطاني المذكور تُـستهلك في أعـمال مكافحـة الإرهـاب.[32] أعتقـد أن هـذا الاتجاه سيستمر لسنوات طويلـة مقبلـة. وهنـاك تطـورات مـشابهة تظهـر في مناطق أخرى من العالم، بما في ذلك بعض الدول التي نجحـت حتـى الآن في تجنب خطر الإرهاب.

إن فهم طموح أي جماعة إرهابية وأهـدافها غالبـاً مـا يتـيح للمحللـين المتخصصين في شؤون الأمن تحديد الرد المناسب. وفي بعض الأحيان، يساعد

هذا الفهم على كشف نقاط الضعف في المجموعة الإرهابية، وبالتالي يمكن استغلال هذه النقاط. ولكن تنظيم القاعدة يبدو أنه لا يحمل أي نوع من الأجندات السياسية، مع أن بعض القياديين الأكثر إدلاء بالتصريحات يتحدثون عن تبني سياسات قائمة على تفسيرهم للإسلام. ويعرف المحللون جيداً مسيرة تطور تنظيم القاعدة خلال الأعوام العشرين الماضية، في سهول أفغانستان وجبالها، عندما ذهبت إلى هناك تنظيمات وجماعات متنوعة وعديدة وانضمت للكتائب "المجاهدة" لطرد القوات السوفيتية. ولكن ليس هناك كثيرون اليوم يستطيعون أن يحددوا بدقة اتجاه التطورات بعد 20 سنة من الآن. وأعتقد أن فكر القاعدة سيبقى فترة طويلة في القرن الحادي والعشرين.

القوات الخاصة والعمليات الخاصة

أصبح عالم الاستخبارات مشاركاً ومتعاوناً على نحو متزايد مع القوات العسكرية الخاصة، ووحدات الشرطة التي تحمي الأمن، والوحدات الأخرى التي تنفذ مهمات محددة. وهذا ليس تطوراً جديداً؛ فعلى سبيل المثال، تدير وكالة المخابرات المركزية قسماً خاصاً يُدعى شعبة الأنشطة الخاصة (SAD) منذ سنوات عديدة.[33] ولكن التنسيق بين الجهات المعنية في هذه العمليات أصبح أكثر شيوعاً اليوم، وليس من المستغرب اليوم أن نجد عناصر استخبارات مرافقين لقوة مكلفة بمهمة خاصة. ولكن هذه المهام تنطوي على المخاطر. وقبل تدخل البريطانيين في الصراع الذي دار مؤخراً في ليبيا، كان هناك فريق من القوات البريطانية الخاصة مع عناصر استخبارات من جهاز إم آي 6 قد هبطوا في الصحراء قرب بنغازي، على أمل إجراء

اتصالات مع المقاتلين في المدينة قبل انطلاق عملية إلامي Operation Ellamy.[34] وقد تم اعتقال البريطانيين بوساطة أفراد ميليشيات محلية، وتمت مصادرة معداتهم، وسبّبت هذه الحادثة إحراجاً كبيراً للندن. ولكن الأهم أن الفريق البريطاني فقدَ شيفرات اتصالات شديدة الحساسية تخص وزارة الدفاع البريطانية.

مع تطور عالم الاستخبارات في السنوات المقبلة، أعتقد أن الحدود ستكون متداخلة وغير واضحة بين عمل الأجهزة المدنية مثل إم آي 6، وأجهزة الاستخبارات العسكرية، والقوات الخاصة. وبالفعل حصلت مجلة **آي سباي** مؤخراً على معلومات عن مشروع في البنتاجون يمكن أن يقود إلى إنشاء أول قوة قتالية مؤهلة شبه عسكرية مكونة من جنود متخصصين وجامعي معلومات استخباراتية. والمؤسسة التي تقف وراء المشروع هي وكالة الاستخبارات الدفاعية (DIA)، مع أن المشروع لا يزال قيد الدراسة، ففي نهاية المطاف فإن هذه القوة ستضم آلافاً عدة من الأفراد، وسيكون لديها القدرة على الانتشار السريع للتدخل في المواقف التي تتطلب عملاً عسكرياً، وجمع معلومات استخباراتية. وربما تصبح هذه القوة نموذجاً تحتذي به دول أخرى في المستقبل.

منذ فترة من الزمن، تقوم الاستخبارات البريطانية – أو ربما الأصح أن نقول الاستخبارات الخارجية "إم آي 6" – باستقطاب الأفراد والموارد من فوجين قويين يمتلكان حوافز كبيرة، هما: القوات الجوية الخاصة (SAS)، والقوات البحرية الخاصة (SBS). والجنود الذين يُسحبون من هذين الفوجين يشكلون وحدة سرية، ويكفي القول إنهم يعملون في حقل خطير

هو حقل "العمليات السوداء" black ops. وليس هناك الكثير من المواد المنشورة التي تصف المهام التي تنفذها هذه الوحدات "الخاصة"؛ ولكن جمع المعلومات الاستخباراتية بوساطة قوات عسكرية مؤشر يدل على أن عملهم، بالضرورة، يتضمن عنصر المخاطرة. ولكن بالنسبة إلى الأغلبية الساحقة من العاملين في الاستخبارات، فإن عملهم عادي ومنهجي وشبيه بالعمل التجاري. ولكن يظل هذا العمل خطيراً في نظر البعض، ولذلك يتم توجيه نصائح إلى عدد كبير من العاملين في هذه المهنة بالمحافظة على سرية مهنتهم، أو على الأقل بأن تظل ضمن دائرة العائلة والزوجة. وهذا أمر منطقي، ويحذّر جهاز إم آي 6 المرشحين الجدد للانضمام إليه بأن إخبار طرف ثالث بأنك تقدمت بطلب للانضمام إلى الجهاز يمكن أن يعرقل إجراءات الطلب أو التوظيف.[35]

نادراً ما يقرأ المرء خبر مقتل عميل أو مسؤول أو موظف استخبارات، ولكن هذه العمليات تحدث باستمرار. وعبر التاريخ، كانت تتم تصفية الجواسيس أو إعدامهم بعد اعتقالهم مباشرة، ولكن كلمة "جاسوس" هي مصطلح عاطفي أي أنه يترافق مع عواطف معينة. ومن المحزن أن وسائل الإعلام، وخاصة في الغرب، تشير إلى أي شخص يعمل لمصلحة أجهزة الاستخبارات بكلمة جاسوس. وهذا غير منطقي. هناك نحو 75٪ من إجمالي موظفي مؤسسات مثل "سي آي أيه" أو "إم آي 6" يشاركون في المهام العامة؛ وهناك أشخاص آخرون يعملون في التحليلات الاستخباراتية والمساندة. وليس هناك سوى عدد قليل من الأفراد يتم توظيفهم فعلاً في جمع المعلومات الاستخباراتية.

السحر الأسود

هناك مادة ضمن حقل الاستخبارات تُعرف باسم "الفنون السوداء أو السحر الأسود"، وهي أحياناً تشمل الجانب الأكثر ظلاماً في عالم الاستخبارات، بما في ذلك الجريمة والاغتيالات. ونادراً ما يقرأ المرء عن موت عنصر استخبارات في أثناء الخدمة الفعلية، ولكن ذلك ليس نادر الحدوث. خلال فترات النزاعات، يتم نشر عناصر الاستخبارات في مناطق حساسة وخطيرة، في محاولة لجمع معلومات مفيدة. في الآونة الأخيرة، أصبح أمراً مألوفاً أن يكون هناك موظفون مدنيون يعملون إلى جانب القوات العسكرية. ويوجد على جدار النصب التذكاري لوكالة المخابرات المركزية 103 نجوم تمثل العناصر الذين ماتوا في أثناء خدمة الوطن. ولكن هذا الرقم مأخوذ من حوادث معروفة وموظفين معروفين. وهناك مئات من العاملين مرتبطون بالوكالة – ومنهم أكثر من 30 موظفاً من شركة الخطوط الجوية الأمريكية Air America التي لم تعد موجودة الآن، والتي كانت تابعة لوكالة المخابرات المركزية – ماتوا في أثناء تنفيذ عمليات.[36] وفي نوفمبر 2011، صرح وزير الخارجية البريطاني ويليام هيج أن أشخاصاً موظفين لدى الاستخبارات البريطانية قُتلوا خلال تأدية عملهم في أثناء تنفيذ العمليات.

هل هو عميل أم موظف؟

العنصر/ الموظف يتم عادة تعيينه بصورة مباشرة في أجهزة الاستخبارات أو الدوائر الحكومية؛ بينما العميل غالباً ما يتم تجنيده واستخدامه لجمع المعلومات أو نقلها. والعميل يمكن أن يتقاضى أجراً أو

عربوناً، ولكنه لا يوضع في جدول رواتب جهاز الاستخبارات. وهناك أنواع عديدة من العملاء؛ من عملاء الاعتراض والتشويش، إلى السعاة البسطاء العاملين في نقل الرسائل. وفي حالات الجاسوسية الأكثر تعقيداً، يمكن لعنصر الاستخبارات أن يقوم بدور العميل (الجاسوس) إذا تم تجنيده من قبل جهاز استخبارات أجنبي. ولكن يجب التنويه إلى أن عدد العملاء الذين يُقتلون أكبر بكثير من عدد الذين يُقتلون من بين الموظفين. وفي مسارح عمليات مثل أفغانستان، تم إعدام عدد كبير من الأشخاص الذين يُشتبه في كونهم جواسيس لمصلحة أجهزة استخبارات غربية، ويُعدّ تنظيم القاعدة وحركة طالبان المنفذَين الرئيسيين لهذه الإعدامات.

إن العدد الدقيق لعناصر الاستخبارات الذين قُتلوا في الخدمة لا يمكن معرفته في يوم من الأيام، ولكن بالنسبة إلى المشاركين في جمع المعلومات الاستخباراتية بطرق متقدمة، فإن عملهم يُعدّ مهنة خطيرة. وما دامت الاستخبارات البشرية (HUMINT) مطلوبة فإن القرن الجديد لن يحمل أي عزاء يخفف عن الذين يعملون في دول أجنبية، أو أولئك الذين يُشتبه فيهم، أو الذين يُلقى القبض عليهم. ولا حاجة إلى القول إن جزءاً كبيراً من المشكلة يتوقف على الظروف الفعلية، وعلى المكان الذي تقع فيه الحادثة. وكُتُبُ التاريخ مملوءة بقصص الجرائم الغريبة التي لم تُحَلّ، وغالباً ما تشمل أشخاصاً من أجهزة الاستخبارات، وملفات الجرائم توضح أن هذا الأمر لا يزال يحدث في صناعة الاستخبارات الحديثة في أيامنا هذه. إن تعقب هذه الحوادث والتحقيق فيها يمكن أن يكونا مهمة صعبة، لأن حالات عديدة من هذه الجرائم تقع ضمن الأشياء المشمولة بقانون الأسرار الرسمية للدول،

وتشمل الاستخبارات. ولكن أود أن أعرض باختصار أربع حوادث وقعت في مدينة واحدة فقط هي لندن، نجد فيها أن تورط أجهزة الاستخبارات شبه مؤكد.

في عام 1969، في ذروة الحرب الباردة، انشق المعارض البلغاري جورجي ماركوف، وهرب من بلغاريا إلى لندن. وجد فرصة ليعمل صحفياً ومذيعاً في هيئة الإذاعة البريطانية "بي بي سي". وكان الكثير من التقارير التي يذيعها يعكس معارضته وكرهه للنظام الشيوعي. في 7 سبتمبر 1978، كان ماركوف ينتظر ليركب حافلة في منطقة جسر واترلو؛ لتأخذه إلى مقر الإذاعة في مبنى "بوش هاوس". وفجأة شعر بألم حاد في فخذه، وكان هناك شخص غريب مرّ قربه، ووكزه بواسطة سيخ المظلة. وفجأة شعر ماركوف بارتفاع حرارة جسمه ومات بعد ثلاثة أيام. وعندما قام خبراء الطب الشرعي بفحص جسمه اكتشفوا حبة صغيرة في فخذه مملوءة بمادة الرايسين. وكان القاتل عميلاً بلغارياً تم استئجاره من قبل جهاز الاستخبارات السوفيتي "كيه جي بي"، وكان الاسم الكودي للقاتل "عميل البيكاديلي".[37]

في عام 2013، أجري تحقيق في موت الضابط السابق في جهازَي الأمن السوفيتي (KGB) ثم الروسي (FSB) أليكساندر ليتفيننكو في لندن. كان ليتفيننكو معارضاً بارزاً للكرملين، وانتقل للعيش في بريطانيا حرصاً على سلامته الشخصية، مع زوجته مارينا نحو عام 2000. في عام 2006، التقى زميلاً سابقاً له في جهاز "كيه جي بي"، في لندن، وشربا الشاي معاً في فندق ميلينيوم. ولسوء حظه، كان هناك شخص قد وضع في شرابه مادة مشعة وقاتلة هي بولونيوم 210؛ وهذه المادة تُستخدم للأغراض العسكرية عادة.

مات ليتفيننكو بعد شهر. في يناير 2013، تم الكشف عن حقيقة أن ليتفيننكو كان في الحقيقة عميلاً يعمل لمصلحة جهاز الاستخبارات البريطاني إم آي 6.

وهناك حادثة وفاة مذهلة أخرى وقعت في لندن، في أغسطس 2010، وطالت عنصراً في جهاز إم آي 6. كان جاريث ويليامز فني حاسوب وشيفرات، وكان قد تم انتدابه من قبل قيادة الاتصالات الحكومية (GCHQ) لمصلحة جهاز إم آي 6. وكان يقيم في منزل آمن تابع للجهاز في منطقة راقية تُدعى بيمليكو. وبعد فشل الجهاز في الاتصال بأسرته، طلب من الشرطة زيارة الشقة. وجد عناصر الشرطة ويليامز ميتاً داخل حقيبة رياضية مقفولة وموضوعة في الحمام. في عام 2012، أصدر الطبيب الشرعي تقريره بأن ثمة "جريمة"، وأن من شبه المؤكد أن موته ناتج عن تدخل طرف ثالث.[38] وحسب معلومات مجلة **آي سباي** فإن ويليامز كان يشارك في عملية اختراق سايبرية.

كان من أغرب حوادث القتل في السنوات الأخيرة حادثة مقتل الملياردير المصري أشرف مروان. كان مروان يعيش في شقة فاخرة في منطقة مايفير في لندن. وكان موته على الأرجح يرتبط بمخطوطة كتاب كان يكتبه، ويذكر فيه تفاصيل السنوات الماضية من حياته وأعماله؛ وكانت مخطوطة الكتاب على وشك الانتهاء. في الحقيقة كان مروان ضابطاً سابقاً برتبة رفيعة المستوى في المخابرات المصرية، ويقال إنه زوّد الموساد بمعلومات استخباراتية حساسة، عشية حرب أكتوبر 1973،[39] إلا أن السلطات لمصرية نفت تلك التهمة عنه. وفي 27 يونيو 2008، اكتشف جيرانه جثته في وضح النهار في مدخل شقته، في مبنى كارلتون هاوس تيراس؛ وعلى ما يبدو سقط

من الشرفة. وكان مروان شبه مشلول، ولم يكن في مقدوره أن يتسلق فوق حافة الشرفة إلا إذا وقف على وعاء نبات زينة كان موضوعاً على الشرفة. لو وجد خبراء الطب الشرعي تراباً على حذائه، لربما كان ذلك يُعدّ دليلاً على الانتحار. ولكن الغريب في الأمر، أن الحذاء اختفى في مختبر الطب الشرعي التابع للشرطة، ولم يُعثر عليه بعد ذلك. والمخطوطة المهمة التي كان يمكن أن تعطي معلومات مهمة عن حياته كعميل مزدوج محتمل، اختفت أيضاً. ولا يزال مصير الاثنين (الحذاء والمخطوطة) محيراً وغامضاً. وذكر شهود عيان ملاحظة أخيرة عن هذه القضية الغريبة أنهم شاهدوا رجلين "بملامح سكان حوض البحر الأبيض المتوسط" يقفان على الشرفة؛ وبعد ذلك لم يُعثر لهما على أثر. وحضر جنازة مروان الرئيس المصري [المخلوع] حسني مبارك، ورئيس جهاز المخابرات المصرية [الراحل] عمر سليمان، وهذا دليل على أهمية مروان.

في النظرة المتأنية والعميقة لأي حادثة يمكن أن يجد المرء – غالباً – سبباً محدداً وراء الموت. ووجود سبب للموت لا يجعل الجريمة مقبولة، ولكنه يكشف هوية الذين أعطوا الأمر بتنفيذ العمل، ولماذا قاموا بذلك. إن الحوادث التي تطال عناصر استخبارات يمكن أن تحدث في أي مكان على سطح كوكبنا. فهل هذه الحوادث مرتبطة بعمليات استخبارات حالية ومشكلات قديمة؟ ربما. كان على أجهزة الأمن في دولة الإمارات العربية العمل بصورة جادة؛ لحل لغز واحد من الاغتيالات الأشد غموضاً في التاريخ، والذي حدث في منطقة الشرق الأوسط. ففي 19 يناير 2010، وُجد أحد أعضاء حركة "حماس" الفلسطينية محمود المبحوح مقتولاً في غرفته

في فندق البستان روتانا في دبي. وكـان يبـدو أنـه مـات بـسبب الاختنـاق، في محاولة لجعل موته يبدو أزمة قلبية. وسـرعان ما كـشفت تحقيقـات الـشـرطة الأولية أن موت المبحوح لم يكن حادثة طبيعية. ويظهـر أن العمليـة قـام بهـا جهاز استخبارات يمتلك شهرة واسعة في مثـل هـذه العمليـات، مـستخدماً مجموعة كبيرة من أسـاليب التجـسس والوثـائق وجـوازات الـسفر المـزورة بتقنيات وجودة عالية جداً. وتوحي تفاصيل العملية ومستوى تنظيمهـا بـأن هذه العملية كان يمكن أن تخترق الإجراءات المضادة لأي دولة. وقد شـارك في العملية نحو 30 عميلاً/ عنصـراً، ودخل بعضهم دولـة الإمـارات بـصفة سياح، وبعضهم الآخر بصفة رجال أعمال،... إلخ.[40]

إن الضجة التي أثيرت بسبب استخدام جوازات سفر وهويات أجنبيـة مزورة، بلا شك، ألحقت الضـرر بالعلاقات الدبلوماسية مع الـدول المعنيـة. في أيرلندا، طُلب من دبلوماسـي إسـرائيلي مغادرة البلاد. وفي أسـتراليا، قـام وزير الخارجية ستيفن سميث باستدعاء السفير الإسـرائيلي. وقال إنه إذا تـم التأكـد مـن أن إســرائيل اسـتخدمت جـوازات سـفر أسـترالية لارتكـاب الجريمة، فإن أستراليا سـتعدّ ذلـك "لـيس عمـلاً صـادراً عـن صـديق". إن استخدام جوازات سفر أجنبية، وإصدار هويات مـزورة جـزء مـن أسـاليب الاستخبارات. وإسـرائيل ليست الدولة الوحيدة التي تجيد هذا الفن. ولكن جهاز الاستخبارات الرئيسـي في إسـرائيل، أي الموساد، يمتلك واحـداً مـن المختبرات المهمة والأكثر إبداعاً في مجال إنتاج الوثائق المزورة.[41]

كما وُجهت تهم إلى إسـرائيل باغتيال عدد من العلماء الإيـرانيين الـذين لهم علاقة بالبرنامج النووي الإيراني. وتل أبيـب لا تنفـي ولا تعـترف بمثـل

هذه الأعمال. ولكن الاغتيال في حقل الاستخبارات ليس تخصصاً محتكراً من قبل أي دولة. وملفات الجرائم، كالتي ورد ذكرها في هذه الورقة، عادة تُرتكب بناءً على دوافع سياسية، وجميعها تحمل هدفاً معيناً، أو أنها تُرتكب بقصد إيجاد رد فعل معين. إن بعض هذه الجرائم بلا شك يُصنف ضمن فئة الحرب النفسية. فعلى سبيل المثال، هناك العديد من العلماء الإيرانيين الذين يعملون في البرنامج النووي يشعرون الآن بالخوف، وانشق بعضهم عن نظام طهران وهربوا خارج البلاد. والشكوك والمخاوف أصبحت واضحة في المنشآت النووية الإيرانية.

تجنيد عملاء استخبارات

إن الحوادث المشابهة تزيد من مخاوف الجمهور وشكوكه تجاه عالم الاستخبارات. وتأتي هذه الحوادث في وقت فائق الأهمية للحفاظ على ثقة الجمهور. ولكن أجهزة الاستخبارات تحاول التعامل مع الناس العاديين، وبعضُ الأجهزة، ومن بينها إم آي 6، تسمح الآن بإعطاء لمحة صغيرة فقط عن عالمها السري. وقبل بضع سنوات كان هذا التطور خارج التصور. بالضرورة يتحتم على جهاز الاستخبارات العمل في بيئة سرية، ولكن هذا لا يعني إبقاء الأبواب مغلقة بشكل دائم. قبل 25 عاماً كان مجرد ذكر كلمة "إم آي 6" من المحظورات في البرلمان؛ ومهما كانت الأسباب والأغراض، كان الجهاز يُعدّ غير موجود على المستوى الرسمي. وبالفعل، كان الكثير ممن يتم تجنيدهم في صفوف الجهاز يأتون من الدوائر التي تُسمى "المؤسسة البريطانية"، ومن بين زملاء أو أصدقاء لقيادة تلك المؤسسة. كانت الأندية

السابقة مثل "نادي إن آند أوت" IN and Out Club في لندن، من الأماكن التي يرتادها خبراء التجنيد في جهاز إم آي 6، حيث كان ضباط الجيش يشربون الخمر ويتناولون العشاء ويقضون أوقات التسلية. الآن تغيرت الأمور. إذ تسمح أجهزة الاستخبارات حول العالم الآن للأشخاص المرشحين للتوظيف لديها باستخدام مواقع معينة على شبكة الإنترنت للبحث عن وظائف، وحتى في دول مثل إيران، نجد أن جهاز الاستخبارات الرئيسي في إيران – وزارة الاستخبارات والأمن الوطني – أنشأ موقعاً على شبكة الإنترنت لهذا الغرض.[42] وكان أحد التصريحات الأولى للوزارة التصريح بأن لديها 30 ألف موظف، وهذا يجعلها "أكبر بكثير من وكالة المخابرات المركزية الأمريكية". وربما كانت المفاجأة الكبرى في عام 2013 نشر إعلان من قبل جهاز الموساد الإسرائيلي عبر موقعه على شبكة الإنترنت، للتقدم إلى وظائف لديه. وهناك جدل حول عدد الأشخاص الذين يتم توظيفهم بهذه الطريقة، وتظل إجراءات المقابلة والتوظيف صارمة جداً. وينصح جهاز إم آي 6 مستخدمي الموقع الذين يبحثون عن وظيفة بهذه الطريقة، بأن الإجراءات يمكن أن تستغرق ثلاثة شهور لإنهاء التدقيق الأمني والتعامل مع الطلب.

شعرت أجهزة الاستخبارات أنها مجبرة بالضرورة على التعامل مع شبكة الإنترنت. ويعتقد المسؤولون أن هذا التطور يجعل جهاز الاستخبارات مرتبطاً بالناس ويتيح للناس، وخاصة الشبان والشابات، فهْمَ أهمية هذا العمل. ومن خلال إتاحة الفرصة للناس العاديين لكي يجدوا وظيفة في هذا

القطاع، ومن خلال إعطاء بعض التفاصيل عن المساءلة الدقيقة فيه، فإن عالم الاستخبارات - كما أعتقد- يساعد نفسه. كما أن معظم مواقع أجهزة الاستخبارات والأمن تتيح لأفراد من الجمهور الاتصال بها، وحتى تقديم "معلومات سرية". وأتوقع في المستقبل القريب جداً أن يبدأ عدد أكبر من الأجهزة ببرامج مشابهة، وربما يتخذون خطوات، بحيث يمكن مشاركة الجامعات والمؤسسات التعليمية الكبرى. ومع أن الجزء الأكبر من العمل في أجهزة الاستخبارات سيظل سرياً، فعلى الأقل يمكن جعل بعض جوانب العمل شفافة.

منذ أحداث 11 سبتمبر 2001، أصبحت مؤسسات مكافحة الجاسوسية ومكافحة الإرهاب، على نحو متزايد، مرنة ومتساهلة في التواصل مع الجمهور، وإلى حد ما مع وسائل الإعلام. إن التعاون ضروري في مجالات عدة، ولا حاجة للمرء إلى أن ينظر إلى أبعد من الأحداث الأخيرة في بوسطن، حيث طلب مكتب التحقيقات الفيدرالي والشرطة المساعدة من الجمهور في إيجاد المجرم الثاني الهارب الذي نفذ تفجيرات الماراثون.[43] وخلال ساعات، نشرت مواقع "إف بي آي" والشرطة، على شبكة الإنترنت صوراً للمشتبه فيهم. وفي بريطانيا وأمريكا، هناك برامج منتظمة للتوعية العامة متعلقة بالإرهاب. ومشاركة الجمهور في تحمل المسؤوليات يمكن أن تساعد أجهزة الأمن، وتحفز الآخرين الذين ربما كانوا مترددين في الماضي في تقديم المساعدة، أو كانوا مرتابين بعض الشيء. إن الأمن ربما يكون ضمن مسؤوليات الموظفين الحكوميين وواجباتهم، ولكن كل فرد في المجتمع يمكن أن يساعد في حماية الأمن.

التهديدات وبؤر الاضطرابات الجديدة

لقد تغير عالم الاستخبارات بصورة جذرية منذ أن فُتحت أبواب مكتب الخدمة السرية في بريطانيا عام 1909. وأشك كثيراً في أن الناس الذين عملوا في هذا المكتب الصغير في البداية كانوا يتصورون مدى الأهمية التي ستنالها مهنة الاستخبارات. ولكن الجزء الأكبر من عملهم قبل مئة عام لا يزال أناس آخرون في هذا الحقل يقومون به حتى اليوم، ولا أرى أي تغيير في الكثير من عناصر عمل الاستخبارات التي ناقشناها في هذه الورقة. وستستمر مهام المراقبة والتجسس، ويبدو أن الحرب ضد الإرهاب ستستمر أيضاً. ولكن سيكون هناك طرق جديدة لجمع الاستخبارات، ونشهد منذ فترة استخدام بعض هذه الطرق: طائرات من دون طيار (UAV) تقوم بأعمال التجسس والاستطلاع؛ والتكنولوجيا المتقدمة المستخدمة في الأقمار الصناعية التي تستطيع قراءة رسالة نصية على هاتف خليوي من الفضاء، وابتكار أجهزة ومعدات تجسس فائقة الصغر، وبالتأكيد أصبحت حقيبة الجاسوس حالياً مثيرة للاهتمام أكثر من حقائب أسلافه.

مراقبة أجهزة الاستخبارات ومساءلتها

إن أحد التطورات الرئيسية التي ظهرت بقوة في حقل الاستخبارات في السنوات القليلة الماضية هو إخضاع الاستخبارات للمساءلة السياسية. هناك دول متقدمة عديدة أصبح لديها الآن هيئات تشريعية تقوم بمهمة مراقبة أنشطة أجهزة الاستخبارات وتقييمها. وأصبحت أجهزة الاستخبارات الغربية في معظمها خاضعة للمساءلة، أمام الوزراء والهيئات المتخصصة ذات

الصلاحية. وعلى سبيل المثال، في بريطانيا يخضع جهاز إم آي 5 لإشـراف وزارة الداخلية، أما جهاز إم آي 6 فيخضع لإشـراف وزارة الخارجية. وكلاهما خاضعان للمساءلة من قبل الوزراء والبرلمان والسلطة القضائية، ويعملان وفق أحكام قانون أجهزة الاستخبارات الصادر عام 1994.[44] ولذلك؛ فإن الوزراء الكبار مسؤولون أمام البرلمان عن تصرفات هذين الجهازين، وعن أعمال جهاز الاستخبارات الثالث المعروف باسم قيادة الاتصالات الحكومية (GCHQ). وبصورة عامة، فإن رئيس الوزراء هو المسؤول الأول، وهو بدوره يتلقى النصائح من قبل منسق الأمن والاستخبارات (SIC). ويشرف منسق الأمن والاستخبارات على الإجراءات والتدابير التي تضمن التنسيق بين أعمال أجهزة الاستخبارات بشكل صحيح. ولدى بريطانيا أيضاً لجنة الاستخبارات والأمن (ISC) التي أُسست عام 1994. وهذه اللجنة تقوم بمراقبة السياسات، والإدارة، والنفقات لجميع أجهزة الاستخبارات البريطانية.[45] كما يوجد في بريطانيا لجنة الاستخبارات المشتركة (JIC)، وهي هيئة تابعة لمجلس الوزراء مسؤولة عن توجيه أجهزة الاستخبارات الرئيسية الثلاثة في بريطانيا. وتصدر لجنة الاستخبارات والأمن تقريراً سنوياً، ويتاح للجمهور الاطلاع عليه.

أعتقد أن آليات الإشراف والمساءلة هذه تعزز ثقة الجمهور. وتضمن قوانين المساءلة أيضاً التزام أجهزة الاستخبارات بالعمل تحت مظلة القانون كما تحدده الحكومة. ومع أن النموذج المذكور آنفاً مطبق في بريطانيا فقط، فهناك أنظمة مراقبة ومساءلة سياسية مشابهة مطبقة في أنحاء مختلفة من العالم. ولكن القوانين في بعض الدول سطحية، أو ليست مطبقة إطلاقاً. ومن

المتوقع أننا في السنوات المقبلة من القرن الحادي والعشـرين، سنرى المزيد من الدول تتبنى قوانين وهيئات لمراقبة أنشطة الاستخبارات. ولكن من المهم ألا يتم فرض القوانين لتحقيق أغراض ومكاسب سياسية، كما أن هـذه القـوانين يجب ألا تتدخل في الواجبات العملياتية لأجهزة الاسـتخبارات، أو تعرقلهـا أو تمنعها. ويتضمن نظام الإشـراف البريطاني قنوات وزارية وقانونية متنوعة لمراقبة أجهزة الاستخبارات الثلاثة (إم آي 5، وإم آي 6، وقيادة الاتـصالات الحكومية) والمؤسسات الدفاعية، بـصورة تـضمن للجميـع القيـام بـدورهم بشكل صحيح.

نماذج مستقبلية للاستخبارات

أدت هجمات 11 سبتمبر إلى إحـداث التغيـير الهـيكلي الأكثـر أهميـة في أجهزة الاستخبارات الأمريكية، وإنشاء مكتب مدير الاستخبارات الوطنيـة (ODNI). إن إنشاء نظام يضمن تدفق المعلومات بصورة مستمرة، وتوزيعها على الأجهزة المعنية، كان من الإجراءات الواجب اتخاذها منذ زمـن بعيـد في رأيي، وخاصة بسبب الطبيعة المعقدة جداً لمجتمع الاستخبارات في الولايات المتحدة. ولكن، حتى مع وجود مثل هذا النظـام، فـإن هـذا لا يـضمن عـدم وقوع أخطاء. في حادثة تفجيرات ماراثون بوسطن، تلقت وكالـة المخـابرات المركزية معلومات من جهاز الأمن الفيـدرالي الروســي (FSB) عـن علاقـة تيمورلنك تسارناييف بإرهابيين معروفين من الشيـشان. وكـان تـسارناييف موضوعاً على لائحة المشتبه فيهم في الولايات المتحدة، وتم إجراء مقابلة معه من طرف مكتب "إف بي آي".[46] ولم يجدوا سـبباً للاشـتباه فيـه بأنـه يـشكل تهديداً كبيراً. وهذه الحادثة تعكس مدى صـعوبة مهمـة التحليـل والاكتـشاف

التهديد في أغلب الحالات. ومع ذلك، أعتقد أن هذا النموذج يمكن أن يُستخدم في السنوات المقبلة ليس للربط بين الأجهزة داخل دولة معينة فقط، بل للتواصل على المستوى الدولي أيضاً، وخاصة في مجال محاربة الإرهاب. ومع أن العديد من أجهزة الاستخبارات تتناحر فيما بينها، وكلٌّ منها يعارض الآخر، فإن محاربة الإرهاب هي الميدان الوحيد الذي نشهد فيه ظهور أساليب جديدة للتنسيق. وهذا التنسيق، يمكن أن يساعد في السنوات المقبلة على إقامة علاقات سياسية جديدة، وتقليل التوترات، والتوسط لإبرام جميع أنواع الاتفاقيات.

ستظل الاستخبارات البشرية النوع الأعلى قيمة بين أنواع الاستخبارات، وخاصة إذا كان يمكن تدعيمها بمصادر دقيقة، أو بيانات يتم جمعها بطرق إلكترونية وغير قابلة للشك. وستظل الاستخبارات الجوية، والبرية، والبحرية، والفضائية، خاضعة لهيمنة القوى الكبرى، مع أنه سيكون هناك دول ناشئة تنضم إلى الولايات المتحدة وروسيا. ولن يكون الفضاء بأي شكل من الأشكال ميداناً محتكراً لأي دولة، ولكنه قد يصبح ميداناً للاستخبارات في المستقبل، نظراً إلى جهود دول مثل إيران وكوريا الشمالية لتسريع برامجها الفضائية.

مستقبل الاستخبارات في القرن الحادي والعشرين

من المتوقع تشكيل تحالف استخباراتي جديد لمعالجة المخاوف الأمنية والاقتصادية. ويتوقف جزء كبير من هذا المشروع على كيفية تطور المشهد السياسي العالمي. كما سيكون هناك عمليات أكثر تركيزاً لجمع

الاستخبارات، نظراً إلى ارتفاع تكاليف إدارة شبكات استخبارات عالمية. وبالتأكيد ستتقلص منظومات الاستخبارات، كالتي يديرها مجتمع الاستخبارات الأمريكي (USIC)، و/ أو سيتم دمج الأجهزة الاستخباراتية. وقد أثبت التاريخ أنه في أوقات الصراع ينمو مجتمع الاستخبارات. وإذا تم إرساء الأمن في مناطق الصراع، فإن ذلك سيترك أثراً في عدد الموظفين في الجهاز الاستخباراتي المعنيّ.

أين سيكون عالم الاستخبارات مع نهاية القرن الحالي؟ إن الجزء الأكبر من الجواب يتوقف على كيفية إدارة الشؤون العالمية من قبل قادة كوكب الأرض. ومع أن أدوات الاستخبارات ستصبح أكثر تطوراً، فإن عنصر التحليل لن يتغير. والتحليل الدقيق لا يمكن إنجازه إلا بوساطة الإنسان، ولكن هذا يتوقف على عوامل متغيرة كثيرة. وستكون الاستخبارات "والمنتَج" (أي المعلومات الاستخباراتية) مهمة أيضاً بالنسبة إلى الناس المكلَّفين بتعزيز السلام في المستقبل بقدر أهميتها اليوم. والاستخبارات هي حقاً سلعة مهمة وحيوية، ودعونا نأمل أن تستخدمها الحكومات بطريقة حكيمة في السنوات المقبلة. فهل ستغير الاستخبارات ملامح القرن الحادي والعشرين، أم أن القرن سيغير عالم الاستخبارات؟

الهوامش

1. إن الأجهزة الأساسية التي تشكل مجتمع الاستخبارات في الولايات المتحدة هي: وكالة المخابرات المركزية (CIA)، ووزارة الدفاع الأمريكية (DOD)، ووكالة الاستخبارات الدفاعية (DIA)، ووكالة الأمن القومي (NSA)، والوكالة الوطنية للاستخبارات الجيوفضائية (NGA)، والمكتب الوطني للاستطلاع (NRO)، ووكالة القوات الجوية للاستخبارات والمراقبة والاستطلاع (AFISRA)، وقيادة القوات البرية للاستخبارات والأمن (INSCOM)، وفوج البحرية للأنشطة الاستخباراتية (MCIA)، ومكتب الاستخبارات البحرية (ONI)، ووزارة الطاقة الأمريكية (DOE)، ومكتب الاستخبارات والاستخبارات المضادة (OICI)، ووزارة الأمن الداخلي للولايات المتحدة، ومكتب الاستخبارات والتحليل (I&A)، واستخبارات خفر السواحل (CGI)، ووزارة العدل (DOJ)، ومكتب التحقيقات الفيدرالي (FBI)، وإدارة مكافحة المخدرات/ مكتب استخبارات الأمن القومي (DEA/ONSI)، ووزارة الخارجية الأمريكية (DOS)، ومكتب الاستخبارات والأبحاث (INR)، ووزارة الخزانة الأمريكية (DOT)، ومكتب الاستخبارات الإرهابية والمالية (TFI).

2. مركز الإمارات للدراسات والبحوث الاستراتيجية، «الحروب المستقبلية في القرن الحادي والعشرين»، المؤتمر السنوي الثامن عشر، أبوظبي، 9-10 إبريل 2013.

3. يقول بعض الأكاديميين إن البداية الحقيقية للاستخبارات البريطانية تعود إلى عهد الملكة إليزابيث الأولى (1558-1603)، وكان رئيس الجواسيس لديها السير فرانسيس ولسنجهام.

4. اسم جهاز الأمن الفيدرالي الروسي هو: Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii (FSB).

5. اسم جهاز الاستخبارات الخارجية الروسي هو: Sluzhba Vneshney Razvedki (SVR).

6. الشيفرة اللغز ENIGMA اخترعها المهندس الألماني آرثر شيربيوس في نهاية الحرب العالمية الأولى، وتطورت فيما بعد لتصبح الآلة الرئيسية لدى ألمانيا لفك الشيفرات في الحرب العالمية الثانية.

7. قيادة الاتصالات الحكومية (GCHQ)، تضم 5,000 موظف، وعدد الموظفين تقديري بناءً على إحصائيات رسمية.

8. تم إنشاء وحدة تنفيذ العمليات الخاصة (SOE) من قبل وزير الحرب الاقتصادية هيو دالتون في 22 يوليو 1940. كما كانت تُعرف أيضاً باسم "جيش تشرشل السري" وباسم "المميزون بشارع بيكر"، حيث كان يوجد مقر قيادة الوحدة في لندن.

9. المخابرات المركزية الأمريكية (CIA) أُنشئت في 18 سبتمبر 1947.

10. يحدد المؤرخون العسكريون فترة الحرب الباردة عادة من عام 1947 إلى عام 1991، وهو عام سقوط الشيوعية في الاتحاد السوفيتي.

11. أزمة الصواريخ الكوبية:

(http://www.jfklibrary.org/JFK/JFK-in-History/Cuban-Missile-Crisis.aspx).

12. تمت مبادلة أربعة عملاء للاستخبارات الغربية مقابل إطلاق سراح 10 عناصر من الاستخبارات الروسية، وتأمين مرور آمن لهم. وكانت أسماء العملاء الأربعة: العقيد سيرجي سكيربال، وإيجور سوتياجين، وألكساندر زابوروزسكي، وجينادي فاسيلينكو.

13. حُكم على جوناثان بولارد بالسجن مدى الحياة في مارس 1987، بعد إدانته بتهمة التجسس. ومن المقرر أن يُطلق سراحه في 21 نوفمبر 2015.

14. تم اعتقال برادليماننج في 26 مايو 2010. وقد اتُّهم بارتكاب جرائم عدة في يوليو 2010. ثم تم تغيير التهم الموجهة إليه لتشمل 22 تهمة، في مارس 2011، ومن بينها انتهاك المادتين 92 و 134 من القانون الموحد للقضاء العسكري، وقانون التجسس في الولايات المتحدة.

15. كان جورج بليك موظفاً في جهاز MI6 من 1944 إلى 1961. لمزيد من المعلومات انظر:
Attorney General vs Blake and Another (2000) UKHL 45; (2000) 4 All ER 385; (2000) 3 WLR 625 (July 27, 2000); (http:// www.bailii.org/uk/cases/ UKHL/2000/ 45.html)

16. تقرير المكتب الوطني للمحاسبة (NAO) في بريطانيا حول الهجمات السايبرية، فبراير 2013.

17. **القيادة السايبرية** الأمريكية مقرها حالياً في وكالة الأمن القومي (NSA)، في فورت ميد ميريلاند. وتشكل حالياً جزءاً من **القيادة الاستراتيجية** الأمريكية.

18. المدخلات الإسرائيلية تم تنفيذها بواسطة وحدة متخصصة في الإلكترونيات العسكرية تُعرف باسم "الوحدة 8200".

19. مصادر مجلة **آي سباي** *Eye Spy*. الضحية شخص إيطالي، يقال إنه كان متورطاً في أنشطة إجرامية. أطلق عليه الرصاص، ولكنه نجا من جروحه. خلال ساعات الليل، تم تغيير الجرعة الدوائية التي يتلقاها بمهاجمة نظام المعالجة الإلكتروني المستخدم في المستشفى من قبل قراصنة من خارج المستشفى.

20. خلال التحقيقات في قضية شين تود في مايو 2013، قال المحامي العام في سنغافورة تاي وي شيونج، إن الشرطة اكتشفت رسالة انتحار موجهة إلى والديه ريك وماري وإلى صديقته التي تُدعى شيرلي سارمينتو، على حاسوبه المحمول. ويعتقد والداه أن الرسالة مزيفة، وطلبا من مكتب التحقيقات الفيدرالي (FBI) التحقيق في القضية. الجدير بالذكر أن شين تود كان يعمل في تطوير مادة نيتريد الغاليوم، وهي مادة لها استخدامات عسكرية وتجارية.

21. تقرير لجنة الدفاع البريطانية، 20 فبراير 2012. كان هناك دليل مكتوب من ديف كليمنس، وهو باحث، في برنامج الأمن الدولي، التابع للمعهد الملكي للشؤون الدولية، في تشاتم هاوس. وحذّر كليمنس بشأن ضرورة "الاحتفاظ بالمواهب"، وقال إن الخبراء السايبريين يتلقون أجوراً أعلى في القطاع الخاص.

22. انظر:

Jamal Al-Suwaidi, *From Tribe to Facebook: The Transformational Role of Social Networks* (Abu Dhabi: ECSSR, 2013).

23. لجنة الاستخبارات التابعة لمجلس النواب الأمريكي، إبريل 2013. جيمس كلابر مدير مكتب مدير الاستخبارات الوطنية (ODNI).

24. تعليقات في تقرير صادر عن لجنة الاستخبارات والأمن في البرلمان، فبراير 2013.

25. برنامج إيشيلون ECHELON: يوجد الآن 5 دول موقعة على الاتفاقية الأصلية المبرمة بين الولايات المتحدة الأمريكية وبريطانيا عام 1946، وهي: بريطانيا، والولايات المتحدة، وأستراليا، ونيوزيلندا، وكندا. ويشار إلى هذه الاتفاقية غالباً بمصطلح "العيون الخمسة" Five Eyes و/ أو AUSCANNZUKUS.

26. تقرير لجنة التحقيق في هجمات 11 سبتمبر:

Final Report of the National Commission on Terrorist Attacks Upon the United States, US Government Printing Office (GPO), July 2004.

27. انظر: *Russia And The West,* BBC documentary, January 19, 2012.

28. توصلت مجلة **آي سباي** إلى أن جهاز الاتصال كان وسيلة لتلقي المعلومات وإرسالها من وإلى عملاء في منظمات غير حكومية مقرها موسكو. ومن المثير للاهتمام أن روسيا بدأت في نوفمبر 2012، بتطبيق قانون جديد يحمل اسم "قانون العملاء الأجانب في المنظمات غير الحكومية". وبشكل أساسي يعني هذا أن أي منظمة غير حكومية في روسيا تتلقى أموالاً من دول أجنبية أو مدعومة من دول أجنبية سوف يتم تسجيلها ضمن فئة "عملاء أجانب". وقد زعم الكرملين في مرات عدة أن واشنطن تدعم بعض المنظمات غير الحكومية بهدف إحداث تغيير سياسي في البلاد.

29. تفجيرات ماراثون بوسطن وقعت في 15 إبريل 2013.

30. الصراع الطائفي في أيرلندا الشمالية غالباً ما كان يمتد ويصل إلى بريطانيا من أواخر الستينيات إلى عام 1998.

31. اتفاقية الجمعة العظيمة الموقعة في بلفاست يوم الجمعة العظيمة، 10 إبريل 1998.

32. إحصاءات جهاز الأمن.

33. تعد دائرة الأنشطة الخاصة (SAD) جزءاً من الجهاز الوطني السري (NCS) التابع للمخابرات المركزية الأمريكية. وغالباً ما تجلب هذه الدائرة عناصر إضافية من القوات الأمريكية الخاصة لإنشاء **مجموعة العمليات الخاصة** (SOG).

34. "عملية إلامي" الاسم الكودي الذي استخدمته بريطانيا في تنفيذ دورها/ عمليتها في الصراع الليبي عام 2011، الذي أسفر عن إطاحة معمر القذافي على أيدي القوات الثائرة.

35. انظر:

(http://www.sis.gov.uk/working-for-us/careersfaqs.html).

36. لمزيد من المعلومات عن شركة الخطوط الجوية الأمريكية انظر الكتاب:

William M. Leary, *CIA Air Operations in Laos, 1955–1974*; (https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/ winter99-00/art7.html).

37. قالت صحيفة **التايمز**، في يونيو 2005، إن المشتبه فيه الرئيسي في عملية اغتيال جورجي ماركوف هو رجل دانماركي من أصل إيطالي، يحمل اسم فرانشيسكو جويلينو.

38. . أظهرت تحقيقات الطب الشرعي فيما يخص وفاة جاريث ويليامز، في مارس 2012، «أن وفاة جاريث كانت غير طبيعية، ويُحتمل أن تكون جريمة مخططاً لها مسبقاً. لقد قُتل جاريث ويليامز بطريقة غير قانونية».

39. تعرف إسرائيلياً بحرب يوم الغفران، وعربياً باسم حرب أكتوبر، 6–25 أكتوبر 1973.

40. عموماً هناك اعتقاد سائد بأن جريمة قتل محمود المبحوح نُفذت بناءً على تعليمات من جهاز الموساد الإسرائيلي.

41. جهاز الاستخبارات والعمليات الخاصة (موساد MOSSAD).

42. وزارة الاستخبارات والأمن (MOIS):
(http://www.legislation.gov.uk/ ukpga/1994/13/contents).

43. خلال ثلاثة أيام من بث صور للمشتبه فيهما الرئيسيين في تنفيذ تفجيرات ماراثون بوسطن، وبعد طلب المساعدة من الجمهور، تم التعرف على الأخوين جوهر وتيمورلنك تسارناييف. وتم إطلاق الرصاص على تيمورلنك وأردي قتيلاً، ثم اعتقل جوهر، وواجه تهماً باستخدام أسلحة دمار شامل.

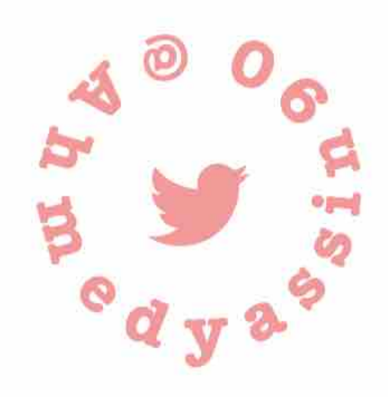
44. قانون أجهزة الاستخبارات 1994:
(http://www.legislation.gov.uk/ ukpga/1994/13/contents).

45. لجنة الاستخبارات والأمن (ISC) أُنشئت بموجب قانون أجهزة الاستخبارات الصادر عام 1994، وهي مكلفة بتحليل السياسات والإدارة والنفقات لأجهزة الأمن، وجهاز الاستخبارات السرية (MI6)، وقيادة الاتصالات الحكومية (GCHQ). وقد قامت هذه اللجنة بتطوير صلاحيات إشرافها بموافقة الحكومة، لتشمل التدقيق في العناصر المتعلقة بالاستخبارات والتابعة لمكتب رئاسة الوزراء: لجنة الاستخبارات المشتركة (JIC)، والإشراف على الموظفين المكلفين بالتقييم، وعناصر الاستخبارات، والأمن، وفريق الرد والتدخل. كما تأخذ هذه اللجنة أدلة من كوادر استخبارات الدفاع (DIS) التابعة لوزارة الدفاع (MOD)، التي تساعد اللجنة فيما يخص العمل ضمن صلاحيات اللجنة. ويقوم رئيس الوزراء بتعيين أعضاء لجنة الاستخبارات المشتركة (JIC) بعد دراسة الأسماء المرشحة من البرلمان، والتشاور مع زعيم المعارضة. وترفع اللجنة تقاريرها مباشرة إلى رئيس الوزراء، ومن خلاله إلى البرلمان، وذلك بنشر تقارير اللجنة. ويخضع أعضاء اللجنة لأحكام القسم 1 (1) (ب) من قانون الأسرار الرسمية لعام 1989، كما يُسمح لأعضاء اللجنة

بالاطلاع على المواد المصنفة بأنها سـرية جداً خلال تأدية واجباتهم. وتأخذ اللجنة أدلة من الوزراء في الحكومة ومن كبار المسؤولين، وتُستخدم جميعها لصياغة التقارير.

46. في عام 2012، كانت قائمة أسـماء الأشـخاص الموضـوعين تحـت المراقبـة الأمنيـة في الولايات المتحدة تضم 730 ألف فرد.



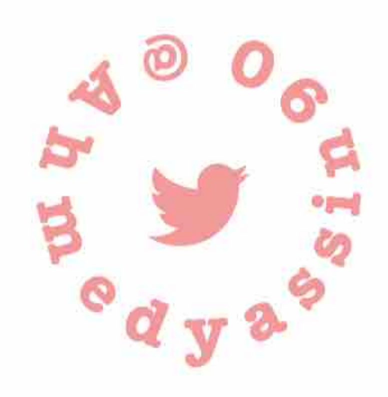

@Ahmedyassin90

نبذة عن المحاضر

مارك بيردسول Mark Birdsall؛ مؤسس مجلة الاستخبارات **آي سباي** *Eye Spy* ورئيس تحريرها، وهي المطبوعة الوحيدة المستقلة في العالم، المتخصصة في شؤون الاستخبارات وجوانبها المختلفة. عمل صحفيَّ تحقيقات ومحللاً وكاتباً في موضوع الجاسوسية لمدة 35 عاماً، وكتب نحو 1500 تقرير عن هذا الموضوع.

منذ إطلاق المجلة المذكورة عام 2000، استخدم بيردسول فريق التحرير والمساعدين المنتشرين في كل أنحاء العالم؛ للتحقيق في أحداث عديدة بدءاً من هجمات 11 سبتمبر 2001، مروراً باغتيال الضابط السابق في جهاز الـ"كيه جي بي" ألكساندر ليتفيننكو في لندن عام 2006. واليوم يبلغ عدد المشتركين في المجلة 500 مؤسسة حكومية دولية، وتُستخدم المجلة كمادة للتدريب والتعليم في العديد من الدورات التدريبية على فنون الاستخبارات، التي تجريها المؤسسات المعنية؛ وهي متوافرة في أكشاك الصحف في أكثر من 50 دولة، ولها جمهور قرّاء حول العالم، ويبلغ نحو 100 ألف قارئ.

وإلى جانب أعمال النشر والتأليف، يعمل بيردسول مع مؤسسات حكومية وعسكرية متنوعة، بحيث يقوم بتعليم "مهنة" التجسس وشرحها، وكذلك تدابير الاستطلاع والمراقبة والتحقيق.


@Ahmedyassin90



169 سلسلة محاضرات الإمارات

مستقبل الاستخبارات في القرن الحادي والعشرين

تصوير
أحمد ياسين

مارك بيردسول



مركز الإمارات للدراسات والبحوث الاستراتيجية